94th Congress
2d Session

COMMITTEE PRINT

SURVEILLANCE TECHNOLOGY -:- 1976

Policy and Implications:
An Analysis and Compendium of Materials

A STAFF REPORT OF THE
SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS
OF THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
NINETY-FOURTH CONGRESS
SECOND SESSION

Printed for the use of the Committee on the Judiciary

94TH CONGRESS
2d Session
COMMITTEE PRINT

SURVEILLANCE TECHNOLOGY

Policy and Implications:
An Analysis and Compendium of Materials

A STAFF REPORT OF THE
SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS
OF THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
NINETY-FOURTH CONGRESS
SECOND SESSION

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
79-064 WASHINGTON : 1976

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price $11.00

PREFACE

In early 1975, soon after I became Chairman of the Senate's Judiciary Subcommittee on Constitutional Rights, I asked the Subcommittee staff to initiate a long-term, comprehensive investigation of the technological aspects of surveillance.

I was concerned about this issue for a number of reasons. First as a Representative and then as a Senator from California, a State known for the number and quality of its high technology centers, I had been exposed for over ten years to the substantial social benefits that derive from our national commitment to innovative technology.

However, as Chairman of the Commerce Subcommittee on Science and Technology and as a member of the Joint Atomic Energy Committee, I was also aware that high technology, if sequestered beyond the reach of evaluation and criticism, tends to develop its own imperatives, some of them potentially damaging to the larger social good, and that "science policy" had gradually disintegrated, becoming an empty slogan, a rhetorical device evoking positive responses but contributing little to the shape of difficult decisions that will profoundly affect the lives of future generations.

My growing sense of unease focused sharply when, as the successor to Chairman Sam Ervin, I assumed major responsibilities for protecting the privacy of individual American citizens. Like many conscientious readers of newspapers and magazines, I had become alarmed about the undeniable and frightening proliferation of technological means to invade a person's privacy, but now I had the duty to act affirmatively.

In commissioning a study of surveillance technology, I reasoned as follows: If knowledge is power, then certainly the secret and unlimited acquisition of the most detailed knowledge about the most intimate aspects of a person's thoughts and actions conveys extraordinary power over that person's life and reputation to the snooper who possesses the highly personal information. And by vastly expanding the range and power of the snooper's eyes, ears and brains, the new technology facilitates and magnifies the acquisition and use of such information. Moreover, as long as surveillance technology remains unregulated and continues to grow at an accelerating rate, the free and enriching exercise of the rights guaranteed by the Constitution and the Bill of Rights will inevitably be chilled to the point of immobility by the general awareness that Big Brother commands the tools of omniscience.

The Subcommittee on Constitutional Rights has held the first three days of projected series of hearings on the topic of surveillance technology. In one sense the report that follows is a status report; it shows what we have learned about the subject to date, drawing upon our own hearings and investigations and upon work conducted in other forums. But in another sense this report goes beyond other efforts in the same genre because it represents a first attempt to organize an immense

amount of data in a comprehensive and usable format and to provide a framework for future analyses and, ultimately, for the creation of institutional mechanisms that will diminish the threats posed by surveillance technology.

It is appropriate that the Introduction to the report begins with references to the conditions now prevailing in the Soviet Union, for it is my hope that by mobilizing and channeling public debate on the costs and benefits of surveillance technology, we can avoid an inertial drift toward the drabness that characterizes life without privacy and liberty.

The design and overall coordination of this report was the responsibility of Douglass Lea, Counsel to the Subcommittee; much of its information comes from the superb staff of the Library of Congress and its Congressional Research Service. Without those resources the report would have been less authoritative and our progress would have been commensurately delayed.

JOHN V. TUNNEY,
Chairman, Constitutional Rights Subcommittee.

CONTENTS

	Page
Preface	III
Introduction	1
CHAPTER I.—OVERVIEW	13
A. Introduction	15
1. Major issues and problems	15
2. Nature and scope of this report	18
3. Definitions	21
B. State of Technology	26
1. Characteristics of today's technology	27
2. Other examinations of the technology	27
a. National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance	28
b. Intelligence and technology	28
3. Categories of surveillance equipment	29
a. Electronic eavesdropping	29
(1) Radiating devices and receivers	29
(2) Nonradiating devices	30
(3) Tape recorders	31
b. Optical/imaging technology	31
(1) Photographic technique	31
(2) Television	31
(3) Night vision devices	31
c. Computers and related technologies	32
d. Sensors	33
e. Other devices and techniques	34
4. Perspectives and prospects	37
C. Congressional action	39
D. Policies and implications of surveillance technology	43
1. Surveillance technology policies	44
a. Scope and magnitude	44
(1) Direct utilization and development	45
(2) Technical assistance and grant support programs	57
(3) Technology transfer	60
(4) Training programs	61
b. Authorities and standards	63
(1) Authorities	63
(2) Standards and guidelies	67
2. Implications of Surveillance Technology	72
a. Constitutional rights of U.S. citizens	73
b. Rights of nonresident aliens and foreign nationals	76
c. Potential conflict of basic rights	76
d. Purposes of surveillance technology utilization	77
e. President's "inherent power" to utilize surveillance	78
f. "Executive privilege"	78
g. Covert versus overt surveillance technologies	79
h. Innovations in surveillance technology	80
E. Controls and oversight	82
1. Ingredients and purposes	82
2. Legislation and proposals	83
3. Congressional oversight	86
4. Federal commission studies	87
5. Executive branch oversight and controls	88

Page

F. Summary and conclusions ... 90
CHAPTER II.—SIGNIFICANT DEVELOPMENTS ... 95
A. Chronology of technological developments ... 97
B. Chronology of administrative and legislative initiatives ... 99
CHAPTER III.—CONGRESSIONAL ACTION AND REACTION ... 103
A. Review of Selected Congressional Hearings and Studies ... 105
Legislative Initiatives ... 106
(1) Omnibus Crime Control and Safe Streets Act of 1968 (P.L. 90-350, Title III; 18 U.S.C. 2511 *et seq.*) ... 106
(2) Fair Credit Reporting Act of 1970 (P.L. 91-508, Title IV; 15 U.S.C. 1681 *et seq.*) ... 106
(3) The Crime Control Act of 1973 (P.L. 93-83; 42 U.S.C. 3771; 40 F.R. 22114 (May 20, 1975)) ... 107
(4) Family Educational Rights and Privacy Act of 1974 (P.L. 93-380; 20 U.S.C. 123g) ... 107
(5) The Privacy Act of 1974 (P.L. 93-579; 5 U.S.C. 552a) ... 107
1. Selected Senate Hearings and Documents ... 111
"Role of the Internal Revenue Service in Law Enforcement Activities." Hearings. Committee on Finance, Subcommittee on Administration of the Internal Revenue Code. (1976) ... 111
"Problems Associated with Computer Technology in Federal Programs and Private Industry—Computer Abuse." Committee Print. Committee on Government Operations. (1976) ... 111
"Privacy—the Collection, Use, and Computerization of Personal Data." Joint Hearings. Committee on Government Operations Ad Hoc Subcommittee on Privacy and Information Systems Committee on the Judiciary. Subcommittee on Constitutional Rights. (1974) ... 112
"Warrantless Wiretapping and Electronic Surveillance—1974." Hearings. Committee on the Judiciary, Subcommittees on Administrative Practices and Procedures and on Constitutional Rights. (1974) ... 113
"Criminal Justice Data Banks—1974." Hearings. Committee on the Judiciary, Subcommittee on Constitutional Rights. (1974) ... 113
"Criminal Justice Information and Protection of Privacy Act of 1975." Hearings. Committee on the Judiciary, Subcommittee on Constitutional Rights. (1975) ... 114
"Federal Data Banks, Computers, and the Bill of Rights." Hearings. Committee on the Judiciary, Subcommittee on Constitutional Rights. (1971) ... 114
"Federal Data Banks and Constitutional Rights." Committee Print. Committee on the Judiciary, Subcommittee on Constitutional Rights. (1974) ... 115
"Military Surveillance" Hearings. Committee on the Judiciary, Subcommittee on Constitutional Rights. (1974) ... 116
"Political Intelligence in the Internal Revenue Service; the Special Service Staff." Committee Print. Committee on the Judiciary, Subcommittee on Constitutional Rights. (1974) ... 116
"Privacy, Polygraphs, and Employment." Committee Print. Committee on the Judiciary, Subcommittee on Constitutional Rights. (1974) ... 117
"Surveillance Technology" Hearings. Committee on the Judiciary, Subcommittee on Constitutional Rights. (1975) ... 118
"Foreign Intelligence Surveillance Act of 1976" Hearings. Committee on the Judiciary, Subcommittee on Criminal Laws and Procedures. (1976) 118
"Electronic Surveillance for National Security Purposes." Joint Hearings. Committee on the Judiciary. Subcommittees on Criminal Laws and Procedures and on Constitutional Rights. (1974) ... 119
"Foreign Intelligence Surveillance Act of 1976." Hearings. Select Committee on Intelligence, Subcommittee on the Rights of Americans. (1976) ... 120
"Presidential Campaign Activities, Final Report." Senate Report No. 93-981. Select Committee on Presidential Campaign Activities. (1974) ... 120
"Governmental Operations with Respect to Intelligence Activities, Final Report." Senate Report No. 94-755. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. (1976) ... 121

Page

2. Selected House Hearings and Documents 122
"Oversight Hearings into the Operations of IRS." Hearings. Committee on Government Operations, Subcommittee on Commerce, Consumer, and Monetary Affairs. (1975) 122
"Access to Records." Hearings. Committee on Government Operations, Subcommittee on Foreign Operations and Government Information. (1974) 123
"Records Maintained by Government Agencies." Hearings. Committee on Government Operations, Subcommittee on Foreign Operations and Government Information. (1972) 123
"Implementation of the Privacy Act of 1974: Data Banks." Hearings. Committee on Government Operations, Subcommittee on Government Information and Individual Rights. (1975) 124
"Interception of Nonverbal Communications by Federal Intelligence Agencies." Hearings. Committee on Government Operations, Subcommittee on Government Information and Individual Rights. (1976) 124
"FCC Monitoring of Employees' Telephones." Hearings. Committee on Interstate and Foreign Commerce, Special Subcommittee on Investigations. (1972) 125
"Dissemination of Criminal Justice Information." Hearings. Committee on the Judiciary, Subcommittee on Civil Rights and Constitutional Rights. (1974) 125
"Surveillance." Hearings. Committee on the Judiciary. Subcommittee on Courts, Civil Liberties, and the Administration of Justice. (1975) 126
"Wiretapping and Electronic Surveillance." Hearings. Committee on the Judiciary, Subcommittee on Courts, Civil Liberties, and Administration of Justice. (1974) 127
"Security and Privacy of Criminal Arrest Records" Hearings. Committee on the Judiciary, Subcommittee on Civil Rights and Constitutional Rights. (1972) 127
"Postal Inspection Service's Monitoring and Control of Mail Surveillance and Mail Cover Programs." Hearings. Committee on Post Office and Civil Service, Subcommittee on Postal Facilities, Mail, and Labor Management. (1975) 128
"Internal Revenue Service Intelligence Operations." Hearings. Committee on Ways and Means, Subcommittee on Oversight. (1975) 129
"IRS Operations and Taxpayer Assistance." Hearings. Committee on Ways and Means, Subcommittee on Oversight. (1975) 129
"Operation Leprechaun." Hearings. Committee on Ways and Means, Subcommittee on Oversight. (1975) 129
"U.S. Intelligence Agencies and Activities, Final Report." House Report No. 94–833. Select Committee on Intelligence. (1976) 130
3. Select Joint Committee Document 131
"Investigation of the Special Service Staff of the Internal Revenue Service." Committee Print. Joint Committee on Internal Revenue Service. (1975) 131
B. Compendium of Congressional Related Materials 132
1. Excerpts from Congressional Documents 134
"The Use of Polygraphs and Similar Devices by Federal Agencies." House Report No. 94–795. House Committee on Government Operations. (1976) 134
Republican Task Force on Privacy. Recommendations. (Congressional Record, v. 120, Sept. 12, 1974) 200
"Space Benefits—the Secondary Application of Aerospace Technology in Other Sectors of the Economy," Excerpts from the Committee Print. Senate Committee on Aeronautical and Space Sciences. (1975) 215
"Investigation into Electronic Battlefield Program," Excerpts from the Committee Print. Senate Committee on Armed Services. Special Electronic Battlefield Subcommittee on the Preparedness Investigating Subcommittee. (1971) 219

Page
2. General Accounting Office Reports 226
"Development of Computerized Criminal History Information System," Excerpts from the GAO Report (1974) 226
"FBI Domestic Intelligence Operations—their Purpose and Scope: Issues that Need to be Resolved," Excerpts from the GAO Report. (1976) 239
3. Congressional Research Service Materials 259
"Computer and Information Security in the Federal Government," Memorandum to Senator Abraham Ribicoff, Chairman of Senate Government Operations, from Louise Giovane Becker. (1976) 259
"Congressional Oversight of Intelligence: Status and Recommendations," Excerpts from the CRS paper prepared by Frederick M. Kaiser. (1976) 269
"Wiretapping and Electronic Surveillance: Federal and State Statutes," Excerpts from the CRS Paper prepared by Christopher Was, M. Elizabeth Smith, and Charles Doyle. (1974) 319
CHAPTER IV.—FEDERAL GOVERNMENT MATERIALS 361
A. Executive Branch 365
Criminal Justice Information Systems (Rules and Regulations) Federal Register, v. 40, May 20, 1975 365
DoJ Guidelies for Domestic Investigations. (March 10, 1976) 383
Electronic Surveillance, Memorandum form William Olson, former Assist. Attorney General for Internal Security to Elliot Richardson, Former U.S. Attorney General, (June 1973) 403
DoJ Standards on Electronic Surveillance Applications, Excerpted from correspondence of Attorney General Edward Levi to Senator Edward M. Kennedy, (June 29, 1975) 425
FCC Memorandum on the Use of Telephone Extension to Monitor Improper Communications; from Dean Burch, FCC Chairman to Representative John Moss (1972) 426
IRS Inspection of Returns by Federal Agencies (1975) 431
IRS Inventory of Mechanical and/or Electronic Devices in custody of the Intelligence Division and Inspection Service's Internal Security Division (1975) 432
Office of Telecommunications Policy. Executive Office of the President. Cable (report to the President). Jan. 13, 1974 (Washington, D.C.) 434
Mail Covers. (Statement by William J. Cotter, Chief Postal Inspector) (1975) 435
B. Commissions 442
U.S. Commission on CIA Activities within the United States, Excerpts from the report of the (1975) 442
Innovations in Intelligence Support, Excerpted from Intelligence Support for Foreign Policy in the Furure. Prepared by Russell Jack Smith. (1975) 449
Science and Technology. Excerpted from Problems in the Conduct of U.S. Foreign Policy: A Compilation of Recent Citations. Prepared by Daniel O'Flaherty. (1975) 452
DoJ Federal Advisory Commission on False Identification. (Proposed Findings and Recommendations, Federal Register, v. 41, June 19, 1976) 453
Electronic Surveillance. Excerpts from the report of the National Wiretap Commission. (1976) 467
Federal Tax Return Confidentiality. Excerpts from the report by the Privacy Protection Study Commission. (1976) 476
C. Courts 486
Application for Orders Authorizing or Approving the Intercept of Wire or Oral Communications, Excerpts from the Report; Director of the Administrative Office of the United States Courts (1966) 486
State of Law of Electronic Surveillance. Excerpts from the National Wiretap Commission Report. (1976) 491

Page

CHAPTER V.—COMPENDIUM OF ADDITIONAL PAPERS AND DOCUMENTS--- 517
A. Review of Technology--- 521
Armer, Paul. Computer Technology and Surveillance, Computers and People, v. 24, Sept. 1975--- 521
ACM Committee on Computers and Public Policy. A Problem List of Issues Concerning Computers and Public Policy, Communications of the ACM, v. 17--- 528
Garvin. Richard. Intelligence and Technology. [Congressional Document] (1976)--- 553
National Wiretap Commission Report, Excerpts from the "State of the Art of Electronic Surveillance." (1976)--- 556
Scoville, Herbert, Jr. The Technology of Surveillance, Society, v. 12, Mar. /Apr. 1975--- 547
B. Civil Liberties Issues and Policy--- 583
American Bar Association. Standards Relating to Electronic Surveillance. (Excerpts) (1971)--- 583
Colby, William. Secrecy in an Open Society. The Center Magazine, v. IX, Mar./Apr. 1976--- 614
Developments in the Law—National Security Interest and Civil Liberties. In Harvard Law Review, v. 85, Apr. 1972--- 627
Kelley, Clarence D. But So is the Right to Law and Order. Trial, v. 11, Jan./Feb. 1975--- 670
Scoville, Herbert, Jr., Is Espionage a Necessary Instrument for Intelligence Gathering? Center Report, v. IX, Apr. 1976--- 673
Sheridan, Thomas I. Electronic Intelligence Gathering and the Omnibus Crime Control and Safestreets Act of 1968. Fordham Law Review, v. 44, Nov. 1975--- 676
Spann, William B. Removing Political Influence from Federal Law Enforcement Agencies. American Bar Association Journal, v. 61, Oct. 1975--- 700
C. United Nations--- 704
"Human Rights and Scientific and Technical Developments: Uses of Electronics which May Affect the Rights of the Person and the Limits Which Should be Placed on Such Uses in a Democratic Society; Report" United Nations Document. (1974)--- 704

APPENDIXES --- 729
A. Privacy Bills Introduced in the 94th Congress; Index and Digests. Compiled by E. Jeremy Hutton, Legislative Attorney, Congressional Research Service, July 14, 1976--- 731
B. Privacy Act of 1974 (Public Law 93–579)--- 805
C. Title 18, Chapter 119. Wire Interception and Interception of Oral Communications--- 820
D. Bibliographies--- 830
1. Computers, Privacy, Government Information and Related Matters, Selected from the CRS Bibliographic Data Base, Jan. 1, 1969–July 15, 1976--- 830
2. Surveillance, Privacy, and Related Items, Library of Congress, MARC Development Office and Information Systems Office, July 1976--- 888

SUBCOMMITTEE ENCLOSURES --- 921
March 16, 1967, from the Washington Post, "Industrial Spies To Turn to Laser Beam, Computer Snooping"--- 923
May 4, 1972, from Jack Anderson's column, "Espionage Equipment"- 923
April 2, 1973, from the Evening Star and Daily News, "That Poodle Could Be a Security Agent," by Michael Satchell--- 924
May 4, 1973, from Jack Anderson's column, "Migraine Weapon"--- 927
June 20, 1973, from the New York Times, "Police to Use TV to Scan Times Square Area for Crime," by Murray Schumach--- 927
July 9, 1973, from the New York Magazine, "Wired City: The Invasion of the Privacy-Snatchers," by Thomas Plate--- 930
July 29, 1973, from the Washington Star-News, "Young's Federal Spotlight—52 of 60 U.S. Agencies Reported Using Bugs," by Joseph Young --- 936

Page

October 14, 1973, from the New York Times, "'Eye in the Sky' Cuts Kansas City Crime" ---- 936
October 18, 1973, from the Village Voice, "Voiceprints—Your Fingerprints Belong to You, But What About Your Voice?" by Larry Lee ---- 938
March 18, 1974, from the Wall Street Journal, "Modern Detection—Police Weapons Range from Electronic Cops to Glowing Bacteria," by G. Christian Hill ---- 942
April 10, 1974, from Computerworld, "X-Ray Machine Probes Brain's Depths" ---- 947
April 11, 1974, from the Los Angeles Times, "Critic of Violence Center Speaks Out," by Isidore Ziferstein, M.D ---- 947
May 30, 1974, from the Washington Post, "Mail and Visitors to Congress Are Now X-Rayed," by George C. Wilson ---- 950
April 8, 1975, from the Washington Star, "Capitol Security: $4.3 Million," by William Taaffe ---- 952
June 4, 1974, from the Manchester Guardian, "Spotting the Truth in a Bead of Sweat," by Simon Winchester ---- 953
August 25, 1974, from the Washington Post, "A.T. & T. Monitors Some Phone Calls," by Ronald Kessler ---- 955
September 1974, from Playboy Magazine, "Bringing the War Home," by David M. Rorvik ---- 957
October 18, 1974, from the New Times Magazine, "Reading the Future" ---- 966
October 31, 1974, from the Wall Street Journal, "Man's Best Friend for Sniffing Bombs May Be a Machine" ---- 967
October 26, 1973, from the Los Angeles Times, "Scramble the Bugs," by Art Seidenbaum ---- 967
November 24, 1974, from the Washington Post, "Thirty Lessons for an Easier Watergate: Do It Yourself" ---- 969
From the Wall Street Journal, "'Debugging' Experts, Aided by Watergate, Detect Rise in Sales," by M. Howard Gelfand ---- 970
March 26, 1975, from the Washington Star, "D.C. Police Plan for Drinking Drivers: A Very Candid Camera," by Toni House ---- 972
March 30, 1975, from Parade Magazine, "FBI's Air Force" ---- 974
January 22, 1974, from the New York Times, "Police Zoom in on Pushers With New Camera Tricks," by Edith Evans Asbury ---- 975
April 10, 1975, from the Los Angeles Times, "23 U.S. Agencies, From Mapping Unit to IRS, Spy on Citizens, ACLU Alleges," by Linda Mathews ---- 976
April 14, 1975, from Newsweek Magazine, "Electronic Fire Spotter" ---- 979
April 24, 1975, from the Washington Post, "U.S. Probes Agents' Role in Wiretaps," by Ronald Kessler ---- 980
June 24, 1975, from the New York Times, "Police Said To Own Devices Illegally" ---- 982
June 26, 1975, from the New York Times, "Private Detectives Are Found To Offer Illegal Wiretap Advice" ---- 983
August 12, 1975, from the Washington Star, "Wiretap Seminar for Police" ---- 984
November 24, 1975, from the Washington Star, "Wiretap School Bared by Paper" ---- 984
From Newsweek Magazine, "New Tools for Cops" ---- 984
June 12, 1975, from New Scientist, "TV Camera for Iran Sees 11 Km at Night" ---- 985
June 12, 1975, from New Scientist, "Machines Dial 999 and Talk to Police" ---- 986
June 19, 1975, from New Scientist, "Semiconductor Scene—Packets of Charge Instead of Currents," by Roy Price ---- 987
July 3, 1975, from New Scientist, "Big Brother Watches Orly Passengers" ---- 990
July 10, 1975, from New Scientist, "Boardroom Electronic Warfare," by Dr. Joseph Hanlon ---- 991
July 10, 1975, from New Scientist, "How We Bugged Commons" ---- 994

Page

July 17, 1975, from New Scientist, "The Telephone Tells All," by Joseph Hanlon 996
July 31, 1975, from New Scientist, "World's Biggest Chip Makes Tiniest TV Camera" 1000
July 31, 1975, from New Scientist, "Fluorescence Fingerprints Exploded Explosives," by Adrian Hope 1001
April 21, 1975, from the Washington Post, "Laser 'Bug' in Nixon Office Reported," by Austin Scott 1001
July 1975, from Penthouse Magazine, "The Spy Among Us," by Tad Szulc 1002
July 7, 1975, from Business Week, "The Erosion of Privacy," by Jethro K. Lieberman 1018
July 12, 1975, from the Washington Post, "Eavesdropping Tools Outflank Law," by Jack Anderson and Les Whitten 1020
June 18, 1975, from the Washington Post, "The Loss of Privacy," by William Raspberry 1021
July 16, 1975, from the Washington Star, "Spying Has Come a Long Way Since the Microphone in the Eagle," by Norman Kempster 1023
July 23, 1975, from the Washington Star, "New Worry: Is the Soviet Listening In?" interview by Orr Kelly 1026
July 31, 1975, from the Washington Post, "'Gun' Mows Down Maryland Speeders," by Alice Bonner 1030
August 4, 1975, from Newsweek Magazine, "True Tales of 'The Other Side'" 1031
August 30, 1975, from the Washington Star, "In Focus—EEG Is Studied as Link Between Man and Machine," by Vernon A. Guidry, Jr. 1033
December 1975, from the Washington Monthly, "The Mind Readers," by Tad Szulc 1036
February 23, 1976, from the Washington Star, "Are Computer Hookups to the Brain Next?" by Cristine Russell 1044
August 4, 1975, from the Washington Star, "Stress Evaluator Reporting—Is It Journalism or Mere Gadgetry?" by Alan Frank 1046
November 7, 1976, from the Washington Post, "The GOP 'Lie Detector'," by Morton Mintz 1050
September 8, 1975, from Newsweek, "No Place To Hide," by Russell Watson with Evert Clark and Anthony Marro 1052
September 14, 1975, from the Atlanta Journal and Constitution, "Military Snooping," by Charles Osolin 1056
November 18, 1975, from the Washington Post, "Long-Distance Phone Calls Found Easy To Intercept," by George C. Wilson 1059
February 13, 1976, from the Washington Post, "Fishing Trip Almost Nets Whopper," by Jack Anderson and Les Whitten 1060
February 19, 1976, from the Washington Star, "Soviet Ships Tap Phones" 1061
February 21, 1976, from the Washington Merry-Go-Round, "Untold Story," by Jack Anderson and Les Whitten 1062
May 10, 1972, from the Washington Merry-Go-Round, "The Strange Secret of 'Operation Pandora'; Russia Poured Microwaves Into Our Embassy; Tried to Brainwash U.S. Diplomats That Way," by Jack Anderson 1063
March 11, 1976, from the Washington Post, "Two Customs Officers Charged in Bugging" 1064
March 19, 1976, from the Washington Star, "Telephone Device Pinpoints Those Personal Calls" 1065
March 19, 1976, from the Washington Star, "Bedroom Bugged, They're Suing for a Million Dollars," by Lurma Rackley 1066
March 19, 1976, from the New Times Magazine, "Spies for Hire" 1067
March 22, 1976, from the New York Times, "Inquiry in FBI Buying Room Surveillance," by Frances Cerra 1068
March 23, 1976, from the New York Times, "Inquiry on FBI's Buying Expanded to All Purchases," by John M. Crewdson 1069
April 9, 1976, from the Times (London, England), "'Skyspy' Can Put Enemy Activities on Television," by Arthur Reed 1070

Page

April 11, 1976, from the New York Times, "Rights Unit Seeks End to Lie Tests," by Peter Kihss 1070
April 15, 1976, from the Wall Street Journal, "The Future Revised—Conventional Warfare Changing Faster Than the Experts Predicted," by Richard J. Levine 1072
April 18, 1976, from the New York Times, "Polygraph Tests Barred CIA Jobs," by Peter Kihss 1076
May 2, 1976, from the Washington Post, "Fifty Thousand Subjected to Legal Wiretaps," by Margaret Gentry 1078
July 3, 1976, from the Washington Post, "The Federal Diary—Abzug Lends Ear on Phone Tapping," by Mike Causey 1079
July 22, 1976, from the Washington Post, "The Age of the Electronic Passport," by Benjamin Welles 1080
July 25, 1976, from the Washington Post, "Big Brother's Sensors," by Paul Dickson 1082
July 27, 1976, from the New York Times, "Olympic Fears Stir Border Patrol Shift," by John Kifner 1086
July 25, 1976, from the Washington Star, "Moss Claims U.S. Wiretaps on Increase" 1087
July 25, 1976, from the Washington Star, "Hill Unit To Appeal on Wiretap Logs" 1089
August 1, 1976, from the Washington Star, "Moss Criticizes Justice on Wiretaps," by Stephen V. Aug 1090
August 8, 1976, from the Washington Post, "The Computer as Couch," by Eric Shulman 1091
August 19, 1976, from the Washington Star, "C&P Puts the Arm on People Dialing 411 for Information," by Mary Ann Kuhn 1097
October 25, 1976, from the Washington Star, "A Former Spy Tells of Being Left in the Cold," by William Beecher 1098
October 26, 1976, from the Washington Star, "A Former Spy Sees a CIA Grown Ineffectual," by William Beecher 1101
October 11, 1973, from the Washington Post, "Electronic Warfare Is a Major Factor in Mideast," by George C. Wilson 1104
January 18, 1974, from the New York Times, "Satellite Films Soviet Space Base," by Theodore Shabad 1106
September 4, 1975, from the Washington Star, "NSA 'Ear' Target of Spy Probe," by Norman Kempster 1107
August 30, 1975, from the New York Times, "National Security Agency Reported Eavesdropping on Most Private Cables," by Nicholas Horrock 1108
June 18, 1975, from the Washington Star, "The New Party Line: Soviets Listen in on U.S. Long Distance Calls," by James Deakin 1111
December 5, 1973, from the Washington Post, "U.S. Tapped Top Russians' Car Phones," by Laurence Stern 1113
December 9, 1973, from the Washington Post, "U.S. Spy Unit Ultra-Secret," by Laurence Stern 1115
February 26, 1976, from the New York Times, "House Panel Calls for Five Contempt Citations in Inquiry on U.S. Surveillance," by Robert M. Smith 1117
April 3, 1976, from the New York Times, "Tapping Computers," by David Kahn 1119
May 12, 1976, from the Washington Star, "In Focus—Spy Satellites Getting Priority in Soviet Space Programs," by Henry S. Bradsher 1121
May 16, 1976, from the New York Times Magazine, "Big Ear or Big Brother?" by David Kahn 1125
August 12, 1976, from the Washington Star, "Church of Scientology Finally Gets Foothold on NSA," by Vernon A. Guidry, Jr 1135
September 10, 1976, from the Washington Star, "In Focus—Two Satellites Revolutionize the Way We Map the Earth," by Thomas Love 1136
September 13, 1976, from the New York Times, "Growing Use of Electronic Warfare Is Becoming a Source of Major Concern for World's Military Powers," by Drew Middleton 1140
December 22, 1973, from the New York Times, "Little Adjustment Needed on Improved TV Camera," by Stacy V. Jones 1141

Page

January 19, 1974, from the New York Times, "Way To Speed Up Taped Speech Legibly Is Devised," by Stacy V. Jones 1142
March 30, 1974, from the New York Times, "First Major Change Made in Color TV Tubes by RCA" 1142
May 16, 1975, from the New York Times, "A Scanning Device for Quick Checks of Credit Invented" 1144
August 9, 1975, from the New York Times, "Computer Setup Links a Variety of Devices," by Stacy V. Jones 1144
October 2, 1976, from the New York Times, "Signature Verification by Computer," by Stacy V. Jones 1145
April 3, 1976, from the New York Times, "Frogman Detector" 1145
October 6, 1976, from the New York Times, "Technology—An Era for Electron-Beam Machines," by Victor K. McElheny 1146
October 30, 1976, from the New York Times, "Patents: Video Memory Is Used in Intrusion-Detection System," by Stacy V. Jones 1147
June 17, 1976, from the Washington Post, "Computer Security Weak, FEA Told," by Donald P. Baker 1148
June 16, 1976, from the Washington Post, "Theft by Computer," by Donald P. Baker 1149
August 2, 1976, from the New York Magazine, "The Computer Did It," by Lori Andrews 1151
August 1, 1976, from the Washington Post, "Convicted Computer Expert Seeks Role as Security Adviser," by Bill Peterson 1154
August 9, 1976, from Newsweek, "The Computer Bandits," by Allen J. Mayer 1155
September 13, 1976, from Time Magazine, "Inside Job" 1157
March 1975, from the Privacy Journal, "Keeping Your Bills Secret in an Electronic Age," by Paul Armer 1157
February 26, 1976, from the Washington Post, "Fed Keeps Hillside Vault," by Charles R. Babcock 1160
February 26, 1976, from the Washington Post, "Funds Switched At Culpeper," by Charles R. Babcock 1163
April 11, 1976, from the New York Times, "Fund Plan Called Peril to Privacy," by David Burnham 1164
August 1, 1976, from the New York Times, "There Was Once Money, Wasn't There?" by David B. Saxe and Dorothy F. Pariser 1166
From the Washington Star, "Electronic Funds Transfer Systems Raise Thorny Issues," by John Holusha 1167
August 4, 1973, from the New York Times, "TV System Aids School Security" 1169
March 10, 1975, from Newsweek Magazine, "Bugging School" 1170
March 25, 1976, from the Washington Star, "Keep Technology for Friends, Pentagon Panel Says," by Henry S. Bradsher 1172
July 13, 1976, from the Washington Star, "Security of Our Schools: Big Business Gets Bigger," by Abbott Combes 1175
September 23, 1976, from the Washington Post, "Electronic Wizards Who Have Something To Crow About," by Robert F. Levey 1176
October 29, 1976, from the Washington Star, "U.S. Approves Strategic Computer Sale to China" 1178
October 30, 1976, from the New York Times, "U.S. Did Not Bar Computer-System Sale to Soviet," by Leslie H. Gelb 1179
1976, winter, from Hastings Constitutional Law Quarterly, volume 3, "Informational Privacy: Constitutional Challenges to the Collection and Dissemination of Personal Information by Government Agencies," by Lawrence J. Leigh 1183
1976, winter, from Hastings Constitutional Law Quarterly, volume 3, "Electronic Visual Surveillance and the Fourth Amendment: The Arrival of Big Brother?" by David P. Hodges 1253
May 1974, from the Privacy Report issued by Project on Privacy and Data Collection/American Civil Liberties Union Foundation, No. 10, "TV: A Two-Way Street" 1254
August 1976, from the Privacy Report, issued by Project on Privacy and Data Collection/American Civil Liberties Union Foundation, volume IV, No. 1, "Private Police in America: The Private Security Industry," by Richard M. Hartzman 1254

Page

September 1976, from the Privacy Report, issued by Project on Privacy and Data Collection/American Civil Liberties Union Foundation, volume IV, No. 2, "Listening In: Governmental Wiretapping and Bugging"---------- 1267
December 9, 1976, from the Washington Star, "U.S. Probes Sale of Confidential Medical Records," by John J. Fialka---------- 1275
December 13, 1976, from the Federal Times, "Microwave Weapons Study by Soviets Cited"---------- 1280

INTRODUCTION

As every man goes through life he fills in a number of forms for the record, each containing a number of questions. . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, buses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence. . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.

—ALEXANDER SOLZHENITSYN, *Cancer Ward*.

And if you consider that they listen around the clock to telephone conversations and conversations in my home, they analyze recording tapes and all correspondence, and then collect and compare all these data in some vast premises (and these people are not underlings), you cannot but be amazed that so many idlers in the prime of life and strength, who could be better occupied with productive work for the benefit of the fatherland, are busy with my friends and me, and keep inventing enemies.

—ALEXANDER SOLZHENITSYN, *Washington Post*, April 3, 1972.

This report, although primarily targeted on the relatively narrow subject of surveillance technology, casts a broader light on social and cultural trends in modern-day America. The picture that emerges is distressing. At its worst, it shows a country at war with its own traditions, a country that fears the logic of its own charter. At its best, it shows a country beginning to grope toward an understanding of the shadowy forces threatening its uniqueness, a country beginning to define the borders beyond which technological and bureaucratic imperatives may not intrude.

From either perspective, the role of the governmental bureaucracy remains distressing. It has developed a life and rationale of its own, an organic separateness that appears anonymous and unresponsive and that often conflicts with democratic goals and with principles of good management. The bureaucracy is skillful in identifying various "threats" and "problems" and in promoting their visibility in a politically attractive way; it is far less resourceful in evaluating its own response to issues and in controlling the money and careers that quickly become vested in the perpetuation of the identified threats and problems.

These characteristics are accentuated in the agencies that contribute to the prevalence of surveillance technology. The goals of the agencies are presented in attractive rhetoric; the means to achieve the ends are shrouded in secrecy; and the results are either selectively embellished for the benefit of the agency or, if unflattering, hidden from outside scrutiny. As a result, funds continue to pour into surveillance technology, and the public is stranded in a Kafkaesque muddle, unable to determine the real means and goals, the real costs and benefits. This result is dangerous when the subject is surveillance technology, for here the marriage between technology and the growth of remote, arbi-

trary power is manifest. Continued ignorance of surveillance technology could prove to be an Orwellian catastrophe for privacy and freedom.

This report attempts to reduce that ignorance by bringing together in one volume the results of pertinent investigations. This report also asks a simple question: What are we doing to ourselves?

Soviet Example

In seeking answers, it may be fruitful to glance first at the Soviet Union, traditionally a negative reference point for Americans wishing to assess trends in their own society.

It takes no more than a glance to realize that personal privacy is not a highly treasured value in the Soviet Union. In their treatment of Alexander Solzhenitsyn and other political and religious dissidents, Soviet officials have made it clear that even the mildest forms of protest may cause massive intrusions into a person's private life. But the antipathy of the Soviet leadership to privacy goes far beyond specific reactions to specific irritations. It is, in fact, part of their political culture, endemic to their way of life, essential to the preservation of their present political system. Invasions of privacy are viewed as necessary fixtures of everyday life, as positive components of the Soviet Union's governing ideology. Thus, all citizens, not only the Solzhenitsyns, who yearn for a measure of personal privacy will be disappointed. For example, in an editorial that appeared on March 31, 1974, *Pravda*, the official Communist Party newspaper, declared that only those who are "morally untidy" worry about privacy. Not content with that, the editorial then decried "Philistine talk about one's private life allegedly being nobody's business," insisting to the contrary that "Party organizations and the public remain indifferent to instances of private property psychology and individualism."

Undoubtedly acting on these values, the Soviet Chamber of Commerce, acting in close cooperation with the Soviet Interior Ministry and the Soviet secret police, the KGB, invited dozens of electronics firms in the United States and other Western countries to exhibit their snooping devices at a Moscow trade fair, called Krimtekhnika '74, in August, 1974.

As the name implies, Krimtekhnika '74 was ostensibly organized to provide a forum for the exchange of technical information and sophisticated hardware in the field of law enforcement and crime control. The Soviet definition of crime, however, is rather flexible. It covers political dissent and thus includes peaceful dissenters like Alexander Solzhenitsyn, Andrei Sakharov and many others, particularly Jewish intellectuals wishing to emigrate from the Soviet Union.

Not content with learning about the criminology of distinguishing between human and animal hairs, the Soviet police officials expressed the greatest interest in viewing the products of U.S. companies that manufacture what are considered to be the world's most sophisticated voiceprint analyzers, lie detectors, identification systems, surreptitious stress analyzers, cameras for night photography and other gear designed to provide authorities with the technological means of intruding into a target's private quarters and private thoughts.

A number of U.S. companies were excited by the prospects of vast new markets for their products. Accordingly, some accepted the Soviet invitations that began circulating early in the Summer of 1974. Others had qualms. The vice president of one firm said, "Some of this equipment could be used against innocent people. It bothers me."

But nothing concerning the fair seemed to bother U.S. government officials. According to one report, an official at the Commerce Department said he had been advised on the Soviet police exhibition by the American Embassy in Moscow. "The embassy recommended that we take a hands-off position if any American businessman contacted us concerning the show," he said. As a manifestation of the government's "hands-off position," the Commerce Department initially claimed that official permission was not required for U.S. companies to show their wares at the Moscow show.

However, when Members of Congress discovered in mid-July that American businesses, most of them heavily subsidized by government contracts, were planning to display their surveillance hardware in Moscow, there was an immediate outcry in both Houses. Senator Henry M. Jackson of Washington, whose Permanent Investigations Subcommittee of the Government Operations Committee was exploring the problems of technology transfer, said the surveillance equipment "could be used to tighten totalitarian control over minorities and dissenting intellectuals." Representative Charles A. Vanik of Ohio said that the display and sale of American surveillance technology "would be like exporting gas chambers to Hitler." Vanik recited passages from Solzhenitsyn's works to illustrate how diligently the Soviet secret police labored in the "Gulag Archipelago" to develop the very technology that was soon to be shipped to Moscow.

As a result of the intense Congressional pressure, the Nixon Administration, then in its final days (thanks in part to its efforts to use a variety of surveillance techniques against American dissenters, political opponents and reputable individuals placed on its "enemies list"), announced on July 19, 1974, the promulgation of new export restrictions to prevent Soviet police from buying sophisticated "personal surveillance" equipment. The Commerce Department said the reason for the U.S. Government's concern was "the welfare of persons who seek to exercise their fundamental rights."

The irony was probably innocent. The Krimtekhnika '74 episode in the Summer of 1974 was quickly forgotten, a brief political squall that soon passed over the horizon. But in fact the episode continues to serve as a paradigm of some of the social and political problems posed by the extraordinary growth and use of surveillance technology.

Lessons of Surveillance Fair

In the episode, for example, it is possible to see the existence of a surveillance technology industry whose principal interests lie exclusively in profit maximization and market expansion. Almost two years later, in April of 1976, a California electronics firm was, in fact, indicted for exporting $3 million in sophisticated electronics manufacturing equipment to the Soviet Union.

The episode, particularly its secret aspects, also casts light on the curious reluctance of the U.S. Government to force the Russians to

halt their microwave bombardment of the American Embassy in Moscow. The bombardment is designed to interfere with American electronic eavesdropping in Moscow, but it has the unfortunate side-effect of jeopardizing the health of American personnel stationed in the Embassy. According to informed sources, the failure to force the issue is caused by the Administration's desire to avoid a detailed public airing of the highly sensitive and esoteric means by which the United States and the Soviet Union intercept important conversations within one another's borders and elsewhere around the world.

Krimtekhnika is not the only example. Shadowy government-to-government dealings in surveillance technology continue:

- In September, 1976, it was revealed that the Swedish government had secretly channeled more than $250,000 over a four-year period to the Chief of U.S. Air Force Intelligence in exchange for electronic surveillance equipment and with the apparent hope that the transaction would escape scrutiny in Sweden and that the U.S. manufacturer would believe that his goods had been sold only to the Pentagon.
- The Shah of Iran has recently signed a multimillion-dollar contract with an American company to create a communications intelligence facility in Iran capable of intercepting military and civilian communications throughout the Persian Gulf area. The contract calls for the American firm to recruit former employees of the National Security Agency and its Air Force component for the project.
- Israel is also bargaining for similar surveillance capabilities, including over-the-horizon radar, heat sensors, magnetic sensors, infrared photographic scopes, light radar scanners that can "hear" the approach of men and vehicles at distances of more than four miles and that can estimate numbers, acoustic sensors to detect tanks or aircraft preparing for action and seismic sensors developed by the U.S. Army in Vietnam and now raised to higher levels of efficiency by the American electronics industry.

In a manner reminiscent of the arms race that began after World War II, the United States seems to be a full participant in, and even the leader of, a new competition between, and a proliferation among, the nations of the world in developing superiority in surveillance technology.

These are some international examples. As this report documents, the same made-in-America surveillance devices can be used against American citizens, with hundreds of millions in taxpayer funds poured into the research, development and dissemination of the technology of social control.

Scope and Findings of Report

This report is an effort to assess the spread of surveillance technology and to shape future investigations and discussions of the costs and benefits.

It is, emphatically, an "interim" report, for the information compiled here, as extensive as it is, can only begin to examine the vast range of issues and problems in public policymaking that fall under the rubric of surveillance technology.

As outlined on the opening day (June 23, 1975) of the series of hearings on surveillance technology held by the Subcommittee on Constitutional Rights, these issues and problems include:

> The Government's role in researching, developing, using and disseminating the technological means of invading privacy and otherwise intruding upon the constitutional rights of American citizens; the adequacy of the Government's present structures and procedures in the area of science policy for assessing the social impacts of new technology that either is designed specifically for surveillance or has derivative surveillance applications; the investment of the taxpayer's dollar to determine whether massive spending on surveillance technology has the effect of wasting scarce public funds and distorting priorities in both the public and private sectors; and the effectiveness of the administration of our present laws, and the possible need for new legislation, to regulate the growth of surveillance technology in both the public and private sectors.
>
> The investigation is unique in its scope. We will approach the problem in its entirety. We will explore the expensive, highly esoteric research and development efforts on advanced computer designs, lasers, satellites, speech processing, image enhancing and others; we will also trace the more prosaic worldwide traffic in cheap electronic eavesdropping devices and ask the responsible Government agencies about what they are doing to regulate this trade. In the process, we intend to look at the practices of Government agencies at all levels and their relationships with private industry, think tanks, and academic research centers.

It was, and remains, an ambitious undertaking. This interim report, which includes a lengthy overview of the subject, numerous texts and excerpts from relevant documents and an exhaustive bibliography, should be viewed from several perspectives: as a definitive set of findings on the structure and scope of the surveillance technology industry; as a statement of the Subcommittee's progress; as an analytic framework for informing future Congressional, Executive and public inquiries into the internal processes and external ramifications of technological advances in surveillance; and as a comprehensive research document that will stimulate and facilitate collateral studies, greater public debate and, finally, coordinated efforts to control or diminish technological threats to Constitutional liberties.

The information that supports the findings of this report has been drawn from a number of sources. The hearings and investigations of the Subcommittee on Constitutional Rights itself is a primary source of relevant information. Under the chairmanships of both Senator Sam J. Ervin, Jr., of North Carolina and Senator John V. Tunney of California, the Subcommittee has probed deeply into the mysteries and perils of computer databanks, lie detectors, wiretapping and bugging practices, military surveillance of civilians and computerized recordkeeping of intelligence files, criminal justice information systems and many other bureaucratic and technological encroachments on the traditional American concept of privacy. The long evolution of these concerns culminated in 1975 when Chairman Tunney initiated a broad series of hearings entitled "Surveillance Technology." Over the past decade many other committees in both Houses of Congress have examined in great depth various pieces of the surveillance technology puzzle. The fruits of those labors are displayed throughout this report. The extraordinary information resources of the Library of Congress give additional weight to the report's findings and recommendations. The report also borrows liberally from various documents produced by the General Accounting Office and numerous Executive Branch departments, offices, commissions and bureaus. Court opinions

and other judicial and legal documents have helped to define the parameters of this report and to point to still-uncharted areas. Finally, significant data have been culled from the avalanche of articles on surveillance technology appearing in the popular and scientific press in recent years.

Yet much of this complex phenemenon remains shrouded in secrecy and jargon. Efforts to obtain authoritative information from the intelligence community are inevitably thwarted on the grounds that even the most circumspect public discussion will undermine the foundations of the Republic by revealing and thereby jeopardizing the essential "sources and methods" of the intelligence craft. The great bulk of the evidence presented in this report casts doubt on this rationale for excluding greater public understanding of the costs and benefits of surveillance technology. In addition, there are already in existence commonly accepted procedures for limited disclosure of government secrets, particularly in legal settings. Moreover, as some of the articles in this report indicate, the intelligence community is highly skilled in the selective leaking of surveillance techniques to the news media when the results are likely to prove self-promoting. Much more plausible explanations for the intelligence community's reflexive hostility toward greater public understanding of its activities are the risks of exposing still more abuses of power and corruption.

At this writing, for example, high FBI officials are being investigated for possible financial corruption involving the use of a Washington, D.C. business, U.S. Recording Co., as a front through which it channeled purchases of electronic eavesdropping equipment in order to disguise the source and nature of the equipment. The question under investigation is whether, because of close personal relationships between the head of the electronics firm and FBI leaders, the company had enjoyed an unfair edge in obtaining the FBI's business, or had been allowed to charge unreasonably high markups for its services or had kicked back money or favors to the FBI personnel. Justice Department officials believe the risks of corruption are high in the area of intelligence, where the law, for reasons of security, allows the intelligence community great latitude in negotiating fees and giving out contracts without competitive bids. Fear of embarrassment and a showing of incompetence may also lie behind the rigid hostility to public scrutiny. And finally, as noted before, the intelligence community is undoubtedly worried about the political consequences of disclosing more information about the extent to which it already enjoys the technological ability to destroy the privacy of innocent American citizens.

Despite the obstacles created by the attitude of the intelligence community, the documents in this report represent in their entirety an instrument by which researchers may triangulate the major themes and activities that result from the intelligence community's commitment to technological surveillance. Thus, although the reasoning that leads to the findings and recommendations of this report may in some instances be more deductive than inductive, the conclusions are all firmly rooted in the documents and references contained in the report.

The findings of this report are hardly reassuring. The report finds that:

- there is indeed a surveillance technology industry;
- the industry is largely unregulated and unscrutinized and, as a result, poses a serious threat to the privacy, liberty and security of every American;
- the key factor determining the continued worldwide growth of the industry is the formal and informal support of the surveillance bureaucracies within the Executive Branch of the Federal Government;
- the Federal Government fails to articulate a coherent national policy on surveillance technology, fails to assess the social, political and economic impact of surveillance technology, and thus fails to provide even rudimentary controls;
- the Congress is precluded from effective oversight of the expenditure of public tax monies in support of the surveillance technology industry by the systemic and pervasive secrecy that cloaks important aspects of its operations;
- new institutional mechanisms need to be developed within the Congress and the Executive Branch to redress the growing imbalance between governmental power based on the technology of surveillance and the Constitutional rights of individual American citizens.

Domestic Surveillance Plague

This report is a product of the evolutionary growth of public dissatisfaction over the steady erosion of personal privacy in the United States and of public fears over the enveloping depersonalization of life in a highly technological society. While public concern has been developing slowly over several decades, it became an explosive political force only after the drumbeat of revelations that uncovered endemic lawlessness in the White House and the intelligence agencies. The constellation of crimes and dubious activities now known as Watergate and the litany of abuses emanating from the intelligence community illustrated exactly what the government can do when its activities are shrouded in secrecy and its vast information resources are applied in a punitive, selective and destructive fashion. Although these manifestations of official arrogance are now part of the national folklore and are firmly embedded in the political culture, it is still not generally understood that they were all motivated by an underlying Faustian thirst to acquire personal information on innocent individuals and that, to an astonishing degree, the quenching of this thirst was aided and abetted through technological means. Indeed, one of the more lasting and positive contributions of these unfortunate episodes may be the effect they have had in highlighting the much broader plague of surveillance that generally infects American society today.

Special Prosecutor

Even the prosecution of the Watergate buggings had elements of "fighting fire with fire." When Archibald Cox assumed the job of Special Prosecutor, he asked the Justice Department to make his office as secure as the most secure offices in the FBI. Cox was concerned that the privacy of his staff, and of their conversations with numerous

officials and former officials, might be invaded by any number of hostile spies, from agents of the government or the President's men to the press.

In the walls enclosing the suite of offices given to Cox on the upper floors of a new building on Washington's McPherson Square, the security officer of the Justice Department installed vibration detectors which would give an alarm if anyone tried to break through from an adjoining suite. Other devices capable of detecting motion were installed over doors connecting different sections of the Special Prosecutor's suite, so that security guards at the entrance could tell, at night, whether anyone was prowling around. Closed circuit television cameras monitored the common hallway, picking up anyone who got off the elevator or who approached the door to the Special Prosecutor's office. Alarm tape was placed on the windows of all offices to detect any effort to break in that way. Staff members were instructed to keep their venetian blinds closed at all times to frustrate efforts to photograph through the windows, and each window was equipped with heavy drapes. Whenever a sensitive conversation was to take place, staff members closed the curtains to prevent the sound waves from their conversations from creating slight vibrations in the window panes, vibrations which could be detected and amplified by eavesdropping equipment employing lasers aimed at the window. The offices were periodically swept for tiny electronic bugs, and the telephone lines were checked for wiretaps. Security guards were on duty 24 hours a day.

Surveillance Environment

The precautions taken at the Special Prosecutor's office, while undeniably expressing the exaggerated paranoia of Watergate, also exemplify on another level what might be called the "surveillance environment." It is a specific reaction to a specified and possible threat. But the cycle is endless: an advance in offensive surveillance equipment generates an equivalent advance in electronic countermeasures.

The "surveillance environment" is rapidly spreading across the landscape. Fully matured technology, whether originally developed for national security purposes, law enforcement applications or space exploration, is not abandoned in dusty warehouses or vacant lots. Too much has already been invested in its development, notably money, time, careers and reputations. If space exploration is curtailed and no longer commands priority treatment, if overseas wars are no longer supported and electronic battlefields are inoperative and if campus and urban riots are no longer common and their threat is relegated to history, then efficient maximization of the investment requires new challenges, new operations and new threats.

Agency Involvement

Already such Federal agencies as the Law Enforcement Assistance Administration (LEAA) and the departments of Health, Education, and Welfare, Housing and Urban Development, Defense, Transportation, the Central Intelligence Agency and the National Security Agency are actively seeking new markets for surveillance devices and promoting the creation of new applications for the basic technology.

LEAA, for example, is considered the prototype for a "new federalism." In practice, this means that the agency's control over how its grant recipients use its money is negligible, even when the Federal funds are used to purchase surveillance devices in the marketplace and even when those purchases are made in states where wiretapping and other forms of surveillance are illegal. Furthermore, LEAA encourages the purchase of the devices by subsidizing the training in their use. Indeed, surveillance schools are flourishing in the wake of the taxpayer's largesse. Over the past five years, LEAA has funded a wide range of activities involving electronic surveillance: blimps and helicopters loaded with electronic gear to trace the movements of suspects on the ground; closed-circuit television monitoring systems; and an endless variety of devices that employ low-light amplifiers, weapons detectors, sensors of all types, X-ray search and voice analysis. According to one news report, the agency provided $50,000 to produce a highly sophisticated viewing instrument designed to look into tight dark spots and refer an image to someone viewing a monitor some distance away. Explained the Director of LEAA's National Institute of Law Enforcement and Criminal Justice: "We don't know what to do with it. We gave the money, the contractor produced exactly what we asked for. It works. But we don't know what kind of problem it can solve. We're looking for a problem now."

The National Institute Director's words should be set in concrete, for they encapsulate the need for new public policies to control surveillance technology. Tax money is appropriated for a popular purpose like law enforcement, an agency turns it over to a private contractor, the contractor produces as promised, and then a problem, or a reason for the whole exercise, is sought. Without effective controls over the process, it is little wonder that the surveillance plague is growing out of control. Indeed, the next step in the process is what a police officer described as "the paint it blue syndrome," whereby the private contractor may alter the design slightly and then market the item independently. At this point there is no guarantee that the device would not fall into the hands of organized crime, or perhaps a jealous spouse or international terrorists.

A former CIA official told the Subcommittee staff that the LEAA viewing device may have been ordered by the CIA, using LEAA as a front. If true, the anecdote further explains the difficulty of achieving public accountability for significant developments in surveillance technology.

Army Technology

Typical of the Defense Department's activities in the field is the Army's "Protection of Key Public Figures" program, created in 1968. Designed to improve protection of the President and other high-level public figures, the program has cost more than $3 million and has thus far produced gun-sniffing miniature poodles, bacteria that glow in the presence of weapons and explosives, hidden X-ray and voice analysis machines and infrared scanners that spot concealed weapons in crowds and instantly pinpoint incoming sniper fire. It is not necessary to discourage such developments if they serve a valid public purpose; it is, however, necessary to know that such developments are occurring and to assess their larger social impacts in order to de-

termine whether their use and dissemination should be regulated to preserve Constitutional rights. The Department of Transportation is active in the dissemination of surveillance devices at airports and/or sensors for the control of traffic along interstate highways. It takes little imagination to see how these sensors could be keyed to track individual automobiles.

Other government agencies and their private contractors are busy developing a range of technologies that will eventually be able to monitor and track anything that moves: computer applications that may eventually eavesdrop on an individual's brainwaves; electronic scanners that can sort through written transmissions and thereby make the surveillance of documents a less expensive proposition; sophisticated scanners that will key to words on tape recordings and thereby drop the manpower costs of wiretapping and bugging; microwave interceptors that can target specific telephone calls; roving wiretaps that use control boxes in telephone exchanges to avoid the expense and effort of physical connections to specific telephone lines; pen registers that can record the numbers dialed from a telephone along with the date, time and length of call; switch and signal wiretapping equipment that can sweep at high speed through thousands of communications circuits per hour searching for special signal address patterns; heat detectors and cameras that can permeate through certain textures and surfaces to distinguish recognizable shapes and movements; microwave respiration monitors that can, from as far away as half a mile, monitor the variations in the movement of a person's solar plexus to determine whether the person is telling the truth; another lie detector that works by monitoring the minute momentary changes in the pupil, retina and focus of the human eye; and many other exotic technologies, some of them using satellites, lasers and advanced computer designs, that are given more extensive treatment in the body of this report and that, if they continue to expand according to their own imperatives, will create in America the "spider's web" world described in Alexandr Solzhenitsyn's *Cancer Ward.*

Peeking In Our Parks

Perhaps the extent of the plague can best be gauged by an article that appeared in an August, 1976, issue of *Sports Illustrated*, a publication not widely renowed for strident advocacy of Fourth Amendment rights:

> By means of an experimental camouflaged infrared beaming device no bigger than a brick, the National Park Service and the Forest Service are now counting the visitors using their woody tracts to determine how many rangers are needed in each area. Just how the device distinguishes between a hiking Sierra Clubber, a wandering moose and a falling tree limb is not clear. In this dehumanizing day, when there is less distinction between real people and deadwood than there should be, perhaps it does not matter.
>
> We are, after all, within a decade of 1984, the fateful year, as forecast by George Orwell, when a Big Brother will be watching everyone. If the Park and Forest Services continue on their present path, by 1984 they will probably have a refined device that can tell a man from a moose, and will have added a voice box to shout instructions to those of us who seek peace in the woods. "Dress up the column! Move it along!" the Voice will shout. "And you there, Second Class Scout Harold Werbley, you left your mess kit back at Station Four."

We dare the parksters and foresters to plant a counter near Walden Pond. Their good intentions notwithstanding, if the ghost of old Henry Thoreau is still around—and we pray God that it is—the evil eye would be smashed to absolute smithereens.

The editors of *Sports Illustrated* would be even more shocked if they fully realized the degree to which what were once primarily conservation agencies have become Federal police forces. This transformation began in 1970, when the Park Service asked for $660,000 in additional funds for law enforcement and began aggressively to train and equip park rangers for police work; in 1976 the Park Service is allocating more than $17 million to "fight crime."

Private Sector

The private sector of the economy is also actively engaged in the creation and marketing of surveillance devices. As noted before, much of the Government's secret research is conducted by private firms. Advertisements placed by electronics firms support much of the law enforcement and defense trade press. For example, a Kodak advertisement for a high-speed data processor and scanner used for fingerprint and mug shot searches carried the following message: "With LEAA funding you can't afford not to get one." Salesmen from these firms and displays of their wares are staples at the conventions of such groups as the International Association of Chiefs of Police, the International Security Conference and even elementary school guards. They participate, along with representatives of the law enforcement and intelligence communities and other interested government, academic and private parties, in large meetings called to discuss such topics as "electronic crime countermeasures." The world of surveillance technology is pervaded by a complex network of personnel interchanges among government agencies, outside corporations, university research staffs and consulting firms. Conflicts of interest are inevitable. Moreover, patents or other property or contract rights seem to travel easily from the public to the private sectors.

The few and fragmentary laws that are in effect and that do offer minimal regulation of the industry are largely ineffective. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the wiretap provision, is seldom invoked, particularly its section against the importation of bugging devices. One writer has observed that Customs inspectors are untrained and therefore unlikely to recognize and confiscate the devices when they enter the country. Cheaply produced bugs can be purchased for as little as $10 under the guide of "baby sitting devices." The National Wiretap Commission surveyed a random selection of 115 private detective firms and discovered that 42 either offered illegal wiretap services or advised where they could be found. If that percentage holds when applied against the national total of 4,280 private detective firms, then 1,498 of them are operating illegally.

Signs of the Plague

During the depths of the recent recession in the economy, the surveillance technology industry remained healthy and expansive. Indeed, the rise in crime that accompanied the downturn became a prima facie reason for the industry's further expansion.

The infection of virtually all segments of American society by the surveillance industry's products is beginning to raise alarms. Needless to say, the Watergate revelations and the intelligence community investigations have caused the most widespread concern. But the concern surfaces in some obscure corners as well. A former CIA operative bitterly tells how his torture in 1965 at the hands of the Egyptian secret police was preceded by the bugging of his Cairo home, apparently with high quality eavesdropping devices provided by the United States to Egypt for use against the Russians. Once surveillance technology begins to circulate in an unregulated fashion, neither the ultimate users nor the ultimate targets can be predicted. Indeed, Justice William O. Douglas wrote in a Supreme Court opinion that he believed both the Supreme Court itself and a President of the United States had been subjected to electronic surveillance. Another writer asserts that President Nixon's Oval Office was bugged by a laser device, probably installed by one of our own intelligence agencies. A national survey finds that 52 percent of the American people agree that "things have become more repressive in this country over the past few years." The President of the Massachusetts Institute of Technology tells the International Communications Association that its members are implicated in the creation of an "information tyranny" that poses a serious threat to the Bill of Rights.

Is America entering George Orwell's nightmare where there is "no way of knowing whether you were being watched at any given moment?" As Orwell observed, "How often, or on what system, the Thought Police plugged in on any individual wire was guess work. It was even conceivable that they watched everybody all the time."

As long as the surveillance technology industry remains largely unregulated, the threat will persist and the question will remain open. If it happens, the American version of this nightmare will arrive without the suddenness of a Pearl Harbor and without recognizable archvillains like Big Brother or Hitler and Stalin. But the terrain will resemble Solzhenitsyn's wasteland, where privacy has no value and freedom is a figment of rhetoric. In America it will arrive on a wave of good intentions, incrementally building on each new set of threats, and administered by "problem solvers." But in 1928 Justice Brandeis warned us clearly: "Experience should teach us to be most on our guard when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."

CHAPTER I

Overview

*A. Introduction**

1. Major Issues and Problems

Surveillance technology and its recent development and growth harbor a series of implications for governmental policy, individual liberties, and constitutional rights. The dilemma inherent in a democratic society—between ensuring internal and national security without jeopardizing the civil liberties of citizens and democratic rights of the society—is reflected in the use and control of surveillance technology. Writing in another context, Abraham Lincoln recognized the fragile and complex balance necessary to maintain both security and liberty:

> Must a government, of necessity, be too strong for the liberties of its own people, or too weak to maintain its own existence?
>
> —Abraham Lincoln, *Message to Congress*, July 4, 1861.

Part of the precarious and complex balance of these two goals is reflected in the dual nature of surveillance technology—that it can be a benefit as well as detriment to supporting basic democratic rights and liberties.

In the United States those fundamental liberties have been articulated for the most part in the 1st, 4th and 5th Amendments to the Constitution, especially the freedom of speech and of press, the right to assemble peaceably and to petition the Government for a redress of grievances, the right to be secure against unreasonable and unwarranted searches and seizures, and prohibitions against self-incrimination. Implied in these explicit constitutional guarantees are the right of privacy and protection against the "chilling effect" of certain surveillance practices and technology utilization.

Fundamental to the American character is the requirement that personal privacy be preserved and protected by law and administrative practices. This same character demands freedom from unwarranted surveillance and the expectation that the individual may participate fully in economic, social, and political activities without fear of reprisal. In light of recent disclosures of government surveillance and surreptitious information-gathering practices, there has been a growing concern that personal freedom and liberties may be limited or eroded.

The overzealous collection of information and the wide proliferation of recordkeeping systems has contributed to an apprehension of the present dimensions of surveillance activities. Furthermore, innovations and certain advances in technology have contributed to the growing concern regarding surveillance and related activities. Some technological developments themselves have created a significant di-

*This chapter was prepared under the direction of the staff of the Senate Judiciary Subcommittee on Constitutional Rights by Frederick M. Kaiser, Analyst in American National Government, and Louise Giovane Becker, Analyst in Information Sciences, of the Congressional Research Service, Library of Congress.

lemma—on one hand, there is a need to encourage the use of modern tools and techniques to protect individuals and protect their rights yet on the other there is a need to guard against the misuse and abuse of those same technological innovations which threaten personal privacy and liberties. Providing adequate safeguards and controls on technology is a complex and difficult problem. It is apparent that the nature of unwarranted surveillance and the necessity to protect personal privacy place special demands in this area and raise unique issues. (These issues are elaborated in Chapter III, "Congressional Action and Reaction," and Chapter V.B., "Civil Liberties Issues and Policy Implications." A further perspective is provided in Chapter V.C., "United Nations Documents.")

While there is considerable difficulty in identifying all the issues, there is an equal problem in adequately measuring and evaluating the impact of surveillance or the threat of such activities on a society. Implied and real threats to personal freedom often cause individuals to limit and restrict the range and dimensions of their involvement in society. A "chilling effect" might occur which limits and restricts full participation on the part of individuals and groups. Such an effect has a secondary and rather significant impact in that unwarranted surveillance may serve to deprive society of creativity and initiatives necessary to deal with complex problems and issues. Surveillance of individuals may also lead to diminished returns in terms of productivity and viable contributions to its stated purposes—protection of national security and/or law enforcement. The fact that there are no definitive data regarding likely costs associated with surveillance technology—research and development, personnel training, implementation, maintenance, security, etc.—nullifies reliable and valid measurement and evaluation in cost/benefit terms.

The potential impact of surveillance and its associated technology may be critical to defining the ingredients of a democratic political system and in differentiating democratic from other political systems. According to Alan Westin, one of the foremost authorities on the subject of privacy and personal freedoms, differences in "patterns of privacy, disclosure, and surveillance" distinguish democratic from totalitarian states.[1]

> The modern totalitarian state relies on secrecy for the regime, but high surveillance and disclosure for all other groups. With their demand for a complete commitment of loyalties to the regime, the literature of both fascism and communism traditionally attacks the idea of privacy as "immoral," "antisocial," and "part of the cult of individualism." This attitude is most strongly expressed in the consolidation phase of a new totalitarian regime. Autonomous units are denied privacy, traditional confidential relationships are destroyed, surveillance systems and informers are widely installed, and thorough dossiers are compiled on millions of citizens. Most important, the individual is not allowed to gain security by conforming without opposition and quietly doing his job. The regime demands active and positive loyalty. These policies, by creating fear and distrust, tend to foster a sense of loneliness and isolation in the citizen; for relief, he turns to identification with the state and its programs so that he may find the satisfactions of affiliation and achievement.[2]

Westin further notes that:

> Just as social balance favoring disclosure and surveillance over privacy is a functional necessity for totalitarian systems, so a balance that ensures strong

[1] Westin, Alan. Privacy and Freedom. New York, Atheneum, 1967, p. 23.
[2] Ibid.

citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life. The reasons for protecting privacy tend to be familiar to citizens of liberal democracies; thus the specific functions that privacy performs in their political systems are often left unexpressed.[3]

Certain technological aspects per se provide additional problems associated with surveillance. Modern technological developments in electronic eavesdropping equipment—e.g., imagery technology, data communications linkages, automated data processing techniques, sensors, and other devices—have contributed to an anxiety that sophisticated technologies may be uncontrollable in a meaningful democratic sense. A corollary implication is that in a technologically advanced society, such as the United States, tools that are essential to normal and common usage can be adapted to surveillance activities. An example might be the sizable amount of records maintained by Government agencies for necessary processing and implementation of legitimate public programs. Some 6,723 records systems, containing 3.8 billion records about individuals, are held by approximately 85 Federal departments and agencies.[4] The potential use (or abuse) of this massive inventory, computerized for accessibility, is as a passive element in surveillance, one intimately related to various communications networks and including descriptions of personal activity, economic condition, and criminal records. Associated problems are the questioning of the reliability and accuracy of such information as well as its disclosure to unauthorized sources or for political purposes.

A further ramification of surveillance technology involves the sheer growth and increased sophistication of the industry and, consequently, its accessibility to an ever-expanding clientele, both public and private. A summary of the historical development of surveillance has been provided by the Senate Subcommittee on Constitutional Rights:

> The rapid development of information-gathering and communications technologies in the latter half of the nineteenth century set the stage for the privacy controversy which followed over a hundred years later. Photography processes and equipment became easier, less expensive and more mobile. Wiretaps were invented with the telegraph in the 1860's. Telephones and telephone-line taps followed, as well as microphones and various sound-recording devices. By the early 1900's, electronic surveillance was an established method of investigation on the part of both police and private detectives . . .
>
> Also in the early decades of the twentieth century, new technologies of recording and assessing individual personality became available. Polygraphs and personality tests began to be used to record and to measure the most intimate recesses of the human personality. Polygraphs (so-called "lie-detectors") were developed as a police tool in the late 1920's. Personality tests, based on the then newly created sciences of psychology and psychoanalysis, gained respectability through their extensive use by the military during World Wars I and II. Such techniques did not arouse much public antagonism in these years of limited application.
>
> At the same time, communications technologies—from the typewriter to new printing processes, to radio and swifter mail service based on faster means of transportation—brought more and more current information into the hands of more and more people. The technologies of information dissemination were themselves developing concurrently with the development of new methods of collecting information. The public response was generally enthusiastic.

---

[3] Ibid., p. 24.

[4] Office of Management and Budget. Executive Office of the President. Federal personal data systems subject to the Privacy Act of 1974. First annual report of the President (for calendar year 1975). Vol. 1, July 1, 1976, p. 2.

By mid-century (1945–1965), the United States was characterized by even more rapid technological advances and increased reliance on "scientific" methods. Electronic surveillance devices became more powerful, more versatile, smaller and cheaper. Polygraphs became an increasingly popular personnel tool among both private and public employers. Personality tests were embraced by many groups and accepted as a routine procedure in schools, industry and government. Communications technologies developed apace. Most important, computers became an integral part of the nation's record-keeping activities.

At about the same time, there was a growing demand for both administrative personnel data and statistical information about individuals. The social service responsibilities of the federal government greatly expanded during the "New Deal" era; and these new madnates stimulated the need for facts on which to base planning, programming and budgeting decisions. In the many cases where the allocation of federal grants was made to depend on the population characteristics of a given area, the collection of highly detailed information about such population groups by the federal and state governments became essential. Added emphasis in the private sector on social and biomedical research began to involve the gathering of much personal data, sometimes shared with a financially supporting federal agency. In the private sector, business concerns began to collect detailed information about many aspects of their operations, paricularly for tax and marketing purposes. During this period, too, a mobile population discovered the convenience of credit cards. The success of the credit reporting industry in marketing information about consumers has given rise to predictions of an efficient "cashless society," and also to apprehension about "financial privacy."

About this same time, computers began to produce noticeable effects on American society. Congressional hearings noted the growing use of automatic data processing by the federal government, and its impact on established patterns of data collection and interagency information sharing. Soon after the Internal Revenue Service adopted computer procedures in 1963, citizens became obliged to indicate their Social Security number on tax forms. By the mid-1960's, too, growing numbers of state and local law enforcement agencies began to automate various aspects of their opertaions, such as fingerprint identification, analysis of crime characteristics, and retrieval of criminal histories. The computerization of consumer reports by the credit industry made "credit checks" on individuals feasible within seconds. The trend towards centralizing and manipulating information, especially personal information, in computerized data banks began to be viewed with apprehension by a growing number of both politicians and private citizens.[5]

Inherent in such developments has been an expanded potential for surveillance in terms of the number of subjects, the extent of information concerning each one, and the number of operators of surveillance devices. Furthermore, miniaturization of surveillance devices, which inhibits detection and lessens the risk of use, serves as an inducement to increased utilization.

2. Nature and Scope of This Report

This report highlights some of the issues and problems associated with surveillance technology in a democratic society. The purpose of this report is two-fold—to provide the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary with a compilation of selected materials which provide analytical information on the topic and to develop a preliminary framework and analysis for understanding the issues and implications associated with surveillance technology. Because of the potential enormity of a projected examination of surveillance technology, this report is limited to public sector

[5] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Federal data banks and constitutional rights: A study of data systems on individuals maintained by agencies of the United States Government. Staff report. 93d Congress, 2d session. 1974. Vol. 1, pp. X–XII.

involvement in the topic and, more precisely, to Federal Government involvement. The private sector, which performs important supporting functions with regard to technology (e.g., research, production, development) and engages in its own surveillance activities utilizing identical technologies, in many cases, cannot be included in this limited examination.[6]

The Subcommittee on Constitutional Rights has maintained a long-term interest in the issues associated with surveillance and its constituent technologies, an interest which spans the Subcommittee's twenty-year existence and a plethora of specific technologies. That activity and concern, described in an earlier Subcommittee report, is an outgrowth of the Subcommittee's jurisdictional concerns with civil liberties and constitutional rights:

> Among the first activities of the Constitutional Rights Subcommittee after its creation at the beginning of the Eighty-fourth Congress, were extensive hearings on "Security and Constitutional Rights." These 1955 hearings which focused on government security-loyalty programs were followed in the Eighty-fifth Congress by subcommittee hearings on "Wiretapping, Eavesdropping and the Bill of Rights" and "Freedom of Information and Secrecy in Government." During the Eighty-sixth Congress the subcommittee renewed hearings on all three of these privacy-related subjects.[7]

The most recent manifestation of the interest of the Constitutional Rights Subcommittee centered on the 1975 hearings on surveillance technology.[8] Chaired by the new Subcommittee chairman, Senator John V. Tunney, the hearings were concerned with a series of related problems:

> The Government's role in researching, developing, using and disseminating the technological means of invading privacy and otherwise intruding upon the constitutional rights of American citizens; the adequacy of government's present structures and procedures in the area of science policy for assessing the social impacts of new technology that either is designed specifically for surveillance or has derivative surveillance applications; the investment of the taxpayer's dollar to determine whether massive spending on surveillance technology has the effect of wasting scarce public funds and distorting priorities in both the public and private sectors; and the effectiveness of the administration of our present laws, and the possible need for new legislation, to regulate the growth of surveillance technology in both the public and private sectors.[9]

In order to assist the Subcommittee on Constitutional Rights, the Congressional Research Service has, upon request, prepared this report on "Surveillance Technology: Policy Implications." The report includes an overview of some of the primary issues relating to surveillance technology and briefly describes the role of the technology which may be applicable to surveillance operations. Further discussion examines the administrative and oversight practices associated with the phenomenon as well as the state of the art. A brief account of the chapters and their content follows.

In this report prepared by the Congressional Research Service, Chapter 1, introduces the major issues and problems, provides an

---

[6] See Harold Wilensky. Organizational intelligence: knowledge and policy in government and industry. New York: Basic Books. 1967.

[7] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Federal data banks and constitutional rights, op. cit., p. XXXIII.

[8] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Committee on Commerce. Special Subcommittee on Science, Technology, and Commerce. Surveillance technology. Hearings, 94th Congress, 1st session, June 28 and Sept. 9, 10, 1975.

[9] Ibid., p. 2.

explanation of scope of the research and definitions of key concepts, reviews the state of the technology and congressional action in the area, assesses the impact of surveillance technology and its implications for a democratic society, including oversight supervision, and lists some summary questions for further investigations.

Chapter II provides two brief chronologies relating to key developments in surveillance technology and to administrative and legislative initiatives surrounding the utilization of such technologies.

Chapter III examines congressional action and reaction. This overview of recent investigations by congressional committees includes a compilation of the topics and agencies examined, the issues which Congress has emphasized, and the legislative initiatives associated with surveillance technology. A survey of specific Senate and House hearings, investigations, and studies follows the introductory review.

These are followed by excerpts from selected congressional documents, General Accounting Office reports, and Congressional Research Service reports, which elaborate on particular issues in the state of the technology, congressional response to surveillance technology and developments, and examination of certain surveillance uses.

Chapter IV provides a collection of excerpts from other Federal Government sources, specifically the executive branch, federal commissions, and the judicial branch. The "Executive Branch" section includes authoritative statements and procedures for electronic surveillance; guidelines for certain security investigations, surveillance practices, and inspection of certain Federal records; and information processing standards. These materials are extracted from administration testimony before congressional committees and executive publications and include statements from the Internal Revenue Service, Department of Justice, Federal Communications Commission, National Bureau of Standards, the U.S. Postal Service, and the Office of Telecommunications Policy in the Executive Office of the President. The section on Federal commissions excerpts and findings, conclusions and/or recommendations of some of the prominent commissions which have to some degree examined aspects of surveillance technology or its policy and implications. Included are the Commissions on CIA Activities within the United States, on Wiretapping, on Privacy, and on the Assassination of President Kennedy, among others. The two contributions in the section dealing with the Judiciary are the 1975 annual report on applications for authorizing electronic surveillance and a review of the state of the law regarding electronic surveillance.

In combination the sections of Chapter IV provide some of the authoritative statements of Federal policy, a compilation of the concern (or lack ot if) expressed by various commissions, and the judicial interpretation of Federal legislation and administration practices relating to the use of surveillance technologies.

The final chapter, Chapter V, is an extensive compilation of articles, reviews, and analysis of the state of the technology, civil liberties and policy implications of surveillance technology, and international repercussions, including a report on human rights by the Secretary-General of the United Nations. The compilation, utilizing recent publications, focuses on newer developments as well as traditional issues in surveillance technology—computers, networking, electronic surveil-

lance technology, proposed standards for electronic surveillance (American Bar Association), secrecy in an open society, extent of surveillance agencies and operations, authorized electronic eavesdropping, use of polygraphs in the private sector, electronic surveillance in intelligence production and internal security, confidentiality and controls over government records, among others.

An appendix provides a listing of privacy and related legislation introduced in the 94th Congress, two bibliographies dealing with surveillance technology and the policy implications, a copy of the Privacy Act of 1974 (P.L. 93–579), and the section of the United States Code which codifies Federal law with respect to wire interception and interception of oral communications (18 U.S.C. 2510 et seq.).

3. DEFINITIONS

One of the perplexing aspects of an investigation of surveillance and surveillance technology is the lack of consistency and precision regarding the definition of related concepts. It is clear that one of the problems confronted by administrators who utilize certain surveillance technologies, legislators who draft proposed statutes to control that utilization, and justices who interpret the constitutionality of those actions and legislation, is the absence of standardized, legal definitions regarding certain critical concepts. This section does not purport to eliminate that problem but simply to provide working definitions of important concepts—surveillance technology, intelligence, national security, law enforcement, and privacy. In discussing these concepts, it is evident that the imprecise meanings (coupled with the novelty and inventiveness of many of the surveillance technologies and the confidential nature of much of its utilization) make legislating in this area relatively difficult. That definitional imprecision and subsequent administrative discretion, however, are some of the principal reasons for analysts to advocate stricter legislative and judicial controls.

For the purposes of this study, surveillance technology has been given a broad working definition to assist in identifying and understanding some of the critical ramifications of its development. Surveillance technology is that technology which permits an expansion and enhancement of an individual's or an organization's capabilities to monitor and examine the activities of other individuals, groups, and collectivities. This meaning includes not only a consideration of specific electronic equipment or apparatus but also any tools or techniques which permit relative intelligence on individuals or collectivities to be collected, stored, and disseminated. Associated with this definition are technological and administrative innovations which affect the surveillance of an individual or collectivity, and the use of surveillance technologies. Implicit in this definition is the potential to invade the personal privacy of individuals. Although that surveillance and the use of the technology may be done surreptitiously, it is not necessarily performed illegally.

Surveillance and surveillance technology have been inherent ingredients in intelligence production and the intelligence function, whether associated with foreign relations and national security or internal security and law enforcement. These critical concepts need further elaboration and definition.

"The intelligence function," according to McDougal, Lasswell, and Reisman,[10] "comprises the gathering, evaluation and dissemination of information relevant to decision-making, and may include prediction based on such information, as well as planning for future contingencies." This widely encompassing definition recognizes that intelligence production might be associated with any enterprise of society, not just government decision-making and policy-making.

Much of intelligence, as it is applied to government activities, is associated with military strategy and tactics, national defense, and/or national security. In this context, intelligence may be defined as the "product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operations and which is immediately or potentially significant to planning.[11] Admiral William F. Raborn, former Director of Central Intelligence, described the concept of intelligence with an emphasis on the process of evaluation and the objective of national security:

"Intelligence," as we use the term, refers to information which has been carefully evaluated as to its accuracy and significance. The difference between "information" and "intelligence" is the important process of evaluating the accuracy and assessing the significance in terms of national security.[12]

National security, however, appears to be a phrase with multiple meanings, based upon its usage in a particular context, and without a standard definition provided in the United States Code, despite its inclusion in several statutes. The interpretations of "national security" range from a narrow meaning of defense against violent revolution and armed intervention to an extremely broad and virtually all-encompassing one, as noted in a 1972 Harvard Law Review analysis:

"National security" is not a term of art, with a precise, analytical meaning. At its core the phrase refers to the government's capacity to defend itself from violent overthrow by domestic subversion or external aggression. But it also encompasses simply the ability of the government to function effectively so as to serve our interests at home and abroad. Virtually any government program, from military procurement to highway construction and education, can be justified in part as protecting the national security.[13]

Apprehension of such an implicitly pervasive definition has been recently noted in a wiretapping decision by the United States Court of Appeals for the District of Columbia:

Over the past several years there has been increasing anxiety and increasing litigation concerning actions which the Executive Branch of our Government has undertaken under the rubric of "national security." Undoubtedly the President, our Chief Executive and Commander-in-Chief of our armed forces, is imbued by the Constitution with vast and indispensable powers for dealing with the vital

---

[10] McDougal, Myres, Harold Lasswell, and W. Michael Reisman. The intelligence function and world public order. Temple law quarterly, vol. 46, No. 3, spring 1973, p. 365.

[11] U.S. Department of the Army, U.S. Department of the Navy, U.S. Department of the Air Force. Dictionary of United States military terms for joint usage. Washington, U.S. Departments of the Army, Navy, and Air Force. 1955, p. 53.

[12] Anon. What's CIA? U.S. News and World Report. vol. 69. July 18, 1966. p. 74.

[NOTE: Further discussion of the national security intelligence agencies is provided in section D of this chapter—Impact of Surveillance Technology. The principal components are the Central Intelligence Agency, the National Security Agency, the military intelligence units, the State Department Bureau of Intelligence and Research, the Energy Research and Development Administration, the Federal Bureau of Investigation Intelligence Division, and entities within the Justice Department and Treasury Department. Source: U.S. Congress. Senate. Select Committee to Study Government Operations with Respect to Intelligence Activities. Final Report, Book VI: Supplementary Reports on Intelligence Activities, April 23, 1976, Senate report No. 94–755, pp. 132–293.]

[13] Developments in the law—the national security interest and civil liberties. Harvard law review, vol. 85. April 1972, p. 1133.

problems generated by our relations with foreign powers, including the duty to protect this country from foreign aggression or subversion. The very existence of such tremendous power, however, renders it susceptible to abuse and endangers those fundamental personal liberties which the Government was instituted to secure for its citizens and whose exercise elevates the nation to a stature worthy of defense.[14]

Congress, along with the Courts, has been concerned with the use of "national security" as a justification of certain executive actions and its succession over the more limited "national defense." An illustration of the difference in terminology and substantial implications involves the government information security classification policy and Executive Order 11652, the most recent policy statement, issued by President Nixon on March 8, 1972. A recent supplementary report from the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (hereafter referred to as Senate select committee on intelligence) provided the following analysis:

While E.O. 10501 (the previous order on classification) used the referent "interests of national defense" to specify its policy sphere, the new order utilizes "interest of national defense or foreign relations" which collectively refer to "national security." Not only is this a broadening of the policy sphere, but the phrase in E.O. 11652 is not harmonious with the statutory provision upon which it is allegedly based. The Freedom of Information Act clause uses the term "interest of national defense or foreign *policy*." [15]

The intelligence units, which utilize surveillance technologies, are involved to some degree in national security as broadly defined. Yet electronic surveillance for national security purposes is exempted from statutory controls, causing some legislators to advocate new legislative strictures. In supporting the Foreign Intelligence Surveillance Act of 1976, one of its co-sponsors, Senator Edward Kennedy, cited the following defense:

The abuses of Presidential power in the surveillance area reached their zenith under the Nixon administration. And yet, electronic surveillance can also be constructive and useful as a carefully limited, circumscribed tool for gathering certain information truly essential to our national defense. Both the importance of wiretapping, and the dangers inherent in such surveillance—government intrusion into the private lives and conversations of Americans and interferences with the Constitutionally protected rights of privacy, association and speech—dictate that the Congress take quick, effective action.

By expressly incorporating into law the requirement of a judicially approved warrant procedure, by explicitly mandating that both the President and his designate certify in writing the need for such surveillance, and, perhaps, most importantly, by limiting the scope of such surveillance, to those persons acting "pursuant to the direction of a foreign power," this legislation seeks to substantitute the carefully prescribed accountability and oversight for the arbitrariness of the past.[16]

---

[14] *Zweibon* v. *Mitchell*, 516 F. 2d 594, 604 (D.C. Cir. 1975).

[15] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities (hereafter referred to as Senate select committee on intelligence). Supplementary reports on intelligence activities. Final report. Book IV: 94th Congress, 2d session, April 26, 1976. Senate Report No. 94–755, p. 346.

[16] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures. Foreign Intelligence Surveillance Act of 1976. Hearings, 94th Congress, 2d session, March 29, 1976, p. 3.

[NOTE: Prior Congressional investigations have noted the abuses of authority inherent in "national security." Senator Sam Ervin, as Chairman of the Senate Select Committee on Presidential Campaign Activities, concluded with the following observation about the activities of certain White House aides involved in what has collectively been referred to as Watergate:

They had forgotten, if they ever knew, that the Constitution is designed to be a law for rulers and people alike at all times and under all circumstances; and that no doctrine involving more pernicious consequences to the commonwealth, has ever been invented

(Continued)

However, this particular proposed legislation has generated opposition and disagreement over the precision and meaning of some of the critical concepts—"foreign power," "clandestine intelligence activities," electronic surveillance" [17]—reflecting the legal perplexities associated with controlling certain surveillance technologies, especially with regard to national security.

Two prominent implications result from the foregoing discussion of surveillance technology as it is associated with national security and related intelligence production. The first is that surveillance technology is utilized by a variety and multiplicity of Federal agencies, which are likely to operate with individualized administrative standards, different legislative guidance and controls, and varying facilities, capabilities, personnel, and training programs. The second implication is that surveillance technology is often utilized under conditions and for purposes which lack precise meaning or standard legal definition.

Surveillance has also been associated with domestic security and law enforcement functions. More than sixty Federal entities conduct law enforcement, defined in terms of police or criminal investigative activities, and range from the prominent agencies, such as the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), and the military police units, to relatively small and/or obscure units, such as the Division of Law Enforcement of the U.S. Fish and Wildlife Service, the Inspection Branch of the Environmental Protection Agency, and the Security and Investigations Division of the Small Business Administration.[18] These units, especially those involved in guard and protective duties, are likely to utilize advanced surveillance technologies, including, but not limited to, polygraphs,[19] closed circuit television monitors, computerized records systems, counter-intrusion sensors, and radiolocation systems.

A final integral concept in a discussion of surveillance technology is the right to privacy. An earlier study by the Senate Subcommittee on Constitutional Rights summarized the modern legal heritage of this right and import for contemporary society.

As a legal concept, an independent right of privacy was first prominently discussed by the renowned Judge Cooley in his *Treatise on the Law of Torts*, originally published on 1879. In discoursing on "The Right of Privacy," Judge Cooley asserted that "The right to one's person may be said to be a right to complete immunity: to be let alone." Then, in 1890, Samuel D. Warren and Louis D. Brandeis published an article, "The Right to Privacy," that was to become a classic—and generated an interest that has burgeoned ever since. The authors

---

(Continued)
by the wit of man than the notion that any of its provisions can be suspended by the President for any reason whatsoever.

On the contrary, they apparently believed that the President is above Constitution, and has autocratic power to suspend its provisions if he decides in his own unreviewable judgment that his action in so doing promotes his own political interests or the welfare of the Nation. As one of them testified before the Senate Select Committee, they believed that the President has the autocratic power to suspend the fourth amendment whenever he imagines that some indefinable aspects of national security is involved. (U.S. Congress. Senate. Select Committee on Presidential Campaign Activities. Final Report. 93d Congress, 2d session. June 1974. Senate Report No. 93–981, p. 1102.)]

[17] U.S. Congress. Senate. Committee on the Judiciary. Foreign Intelligence Surveillance Act of 1976. Report together with additional and minority views (to accompany S. 3197). 94th Congress, 2d session. July 15, 1976, pp. 68, 71–72, 129–137.

[18] For a listing of Federal agencies performing police and investigative activities, their manpower and budgets, see U.S. Congress. Senate. Committee on Government Operations. Budgetary, organizational, and personnel data on departments and agencies performing police or investigative activities. (A report to the Committee by the Washington Regional Office of the General Accounting Office). 94th Congress, 1st session, 1975.

[19] U.S. Congress. House. Committee on Government Operations. The use of polygraphs and similar devices by Federal agencies. Report. 94th Congress, 2d session, Jan. 28, 1976. House Report No. 94–795.

were inspired by personal outrage over frequent abuses by a then novel breed of snooper—the photographer, professional and amateur. Warren and Brandeis were concerned about non-governmental invasions of privacy and the right of an aggrieved individual to sue for damages another person who has invaded his privacy . . .

It took the scientific and technological revolutions of this century, together with the trend toward centralizing more and more power in government, to bring the privacy issue to the fore. In other words, it was the greatly increased governmental capacity to create massive Federal data banks containing intimate details about the personal lives of individuals, which raised the issue of the impact of these data banks on constitutional rights as a major social and political concern.[20]

The right of privacy involves two distinguishable aspects: 1) the "right to be let alone," which suggests that certain surveillance practices and technology utilization might be prohibited, and 2) the "right to control information about oneself," which assumes the legitimacy of the actual collection of information.[21] This latter aspect is implicit in the definition advanced by Alan Westin: "The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." [22]

The right of privacy defined in the sense of being left alone was reflected in the dissenting opinion of Justice Louis Brandeis in *Olmstead* v. *United States*, 277 U.S. 438 (1927), in which the majority opinion supported Federal wiretapping. Justice Brandeis recognized the inherent potentialities of innovative surveillance technologies and his prophetic dissent is worth quoting at length:

This Court has repeatedly sustained the exercise of power by Congress, under various clauses of that instrument, over objects of which the Fathers could not have dreamed. . . . We have likewise held that general limitations on the powers of Government, like those embodied in the due process clauses of the Fifth and Fourteenth Amendments, do not forbid the United States or the States from meeting modern conditions by regulations which "a century ago, or even half a century ago, probably would have been rejected as arbitrary and oppressive". . . . Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world. . . .

When the Fourth and Fifth Amendments were adopted, "the form that evil theretofore had taken," had been necessarily simple. Force and violence were then the only means known to man by which a Government could directly effect self-incrimination. It could compel the individual to testify—a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life—a seizure effected, if need be, by breaking and entry. Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments, by specific language. *Boyd* v. *United States*, 116 U.S. 616, 630. But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. . . .

The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain,

---

[20] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Federal data banks and constitutional rights : a study of data systems on individuals maintained by agencies of the United States Government. 93d Congress, 2d session, 1974, pp. IX–X.

[21] Hanus, Jerome. Informational privacy. In Stephen Wasby (ed.). Civil liberties : policy and policy-making. Lexington, Massachusetts : D.C. Health, 1976. pp. 119 and 123.

[22] Westin, Alan. Privacy and freedom. New York : Atherton, 1967, p. 7.

pleasure, and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.

Applying to the Fourth and Fifth Amendments the established rule of construction, the defendant's objections to the evidence obtained by a wire-tapping must, in my opinion, be sustained. It is, of course, immaterial where the physical connection with the telephone wires leading into the defendant's premises was made. And it is also immaterial that the instrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficient. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning, but without understanding.

The principle behind the Brandeis dissent finally prevailed forty years later in *Berger* v. *New York* (388 U.S. 41) and *Katz* v. *United States* (389 U.S. 347). (A thorough review of the Supreme Court rulings regarding surveillance technologies, especially electronic surveillance and wiretapping, is found in Chapter III.B.3, in the Congressional Research Service report on "Wiretapping and Electronic Surveillance" and in Chapter IV.C. in the Wiretap Commission report on the "State of the Law of Electronic Surveillance.")

Rather than offer definitive interpretations of key concepts, this section has revealed the absence of precise and standard legal definitions for several, most critically "national security." Furthermore, some of the concepts have fluctuated in their meaning over time or across different contexts, whereas others (e.g., "privacy") are relatively recent constructions in a judicial sense. It is also evident that different surveillance technologies as well as their utilization have import for the different interpretations of a related concept. For instance, the right of privacy may mean the "right to be left alone" when applied to the technology of warrantless wiretapping and the collection of certain types of information (e.g., criminal records) but may mean "the right to control information about oneself" when applied to an individual's access to his own records and restrictions on their dissemination. Finally, the development of working definitions has suggested the widespread surveillance capacity of the Federal Government. The more than thirty units which have a clear intelligence capability plus an additional sixty-five units which conduct surveillance as related to their police and law enforcement responsibilities comprise an imposing number.

B. State of Technology

The technological developments of the past three decades have provided the basis for recent innovations in surveillance technology. Some of the tools and techniques developed in World War II and refined in the post-war era have been surpassed by the technological advances employed in the Vietnam War. The non-military use of some of the technology has been encouraged by the law enforcement and criminal justice community. This section examines some of the devices that have

relevance to surveillance operations and activities. It is not meant to be comprehensive but rather provide an initial framework for understanding the role of technology in surveillance operations.

1. Characteristics of Today's Technology

The revolution in surveillance equipment and related technological developments has been in part a direct result of recent innovations in electronics. The marked diversity and flexibility of electronic systems are often to be found in many of the devices used in surveillance. Much of the technology has some common characteristics which have contributed toward its acceptance and usage. Among these characteristics are:

a. *Miniaturization.*—A key factor that has stimulated wide acceptance of technological innovations has been the development of small, light-weight devices which are often portable. This feature allows the equipment to be easily concealed and permits complexity in circuit development while providing improved functioning.

b. *Quality.*—The higher reliability and sensitivity of the equipment has been possible through overall quality and performance standards. The upgraded equipment function has allowed greater reliance and improved levels of performance.

c. *Processing.*—Operational features have been improved to permit quicker processing times and real time functioning has greatly enhanced surveillance technologies. In many instances the devices and equipment operated without any noticeable lag in processing time. This feature permits instant monitoring and quick access to information.

d. *Cost.*—Improved manufacturing processing with relatively low use of materials has contributed to the economical production of many of the surveillance devices. The economic factors have greatly contributed to the wide acceptance of surveillance equipment and also permitted additional features to be added to surveillance systems at nominal costs.

e. *Other Features.*—Combined with these factors are some additional features that have increased and improved performance of surveillance devices. One aspect that has provided an added dimension to technology has been modularity and flexibility of systems. Modular systems can be incrementally expanded and augmented quickly and relatively easily. A related feature has been the automatic activation of devices and equipment. For example, a sensing device is added to a tape recorder so that it is activated automatically by human voice.

Another critical development is the lack of physical interfaces or visible connections. This permits effective remote monitoring and activation of surveillance equipment. These are but a few of the features that have contributed to wide acceptance of the technology.

2. Other Examinations of the Technology

The continuing concern that recent techonological developments would further erode personal privacy and permit greater surveillance

of individuals and groups has stimulated interest in a special group of equipment and devices. While over the years there has been a consideration of various aspects of this complex issue, the focus more recently has turned to the implications of technology. Congress has examined some of the issues and problems and the concern with the technological developments and the potential for misuse has been debated. (See Chapter III.) In recent years specific attention has been given surveillance technology in light of the revelations of the intelligence community's involvement with domestic surveillance. In addition, the studies by various government commissions are coming to focus on the technological innovations that may have a potential impact on privacy and surveillance activities.

Two recent examinations, excerpts of which are included in this compilation of materials (Chapter V.A, Review of the Technology), deserve explicit mention:

a. *National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance.*—The final Commission study, "State of the Art of Electronic Surveillance," was prepared by John S. Van Dewerker, Asby & Associates, and released in 1976. The study examined five areas—eavesdropping equipment, countermeasures equipment, penetration of other information handling systems, and some of the future systems.[23] Some of the terminology and introductory remarks of the report are included in Chapter V, Section A, "A Review of the Technology."

b. *Intelligence and Technology.*—The Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities also examined some of the problems associated with intelligence-gathering activities and the implications of technological innovations. A 1976 study entitled "Intelligence and Technology," prepared by Dr. Richard Garvin at the request of the Select Committee, reviewed some of the technological implications. (The full text of the report is included in Chapter V, Section A, A Review of the Technology). The report discusses some of the methods of intelligence and information-gathering using the existing technology and focuses on two different techniques:

(1) Covert observation and interception using hidden microphones and cameras and the interception of domestic microwave relay; and

(2) File technology which in the report refers to the use of computerized files to permit surveillance. For example, airline and hotel reservation systems as well as open source literature searches of the New York Times Information Bank are all possible intelligence-gathering information mechanisms. The text search capability and the text editing systems are examined as ways in which the technology can be used in surveillance operations.[24]

---

[23] U.S. National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. State of the Art of Electronic Surveillance. [Washington, 1976], p. 143.

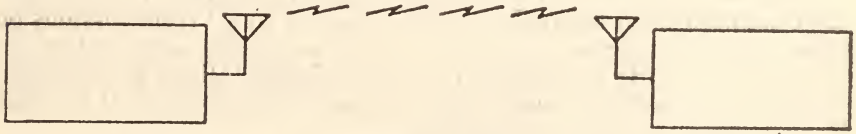
[24] U.S. Congress. Senate. Select Committee to Study Government Operations with Respect to Intelligence Activities. Final report, supplementary detailed staff reports on foreign and military intelligence: Book IV. 94th Congress, 2d session, April 23, 1976. Senate Report No. 94–755, pp. 109–119.

3. Categories of Surveillance Equipment

The main stimulus for the development of innovative equipment and techniques stems in part from the increased legitimate use of surveillance technology. Recent technological advances have also contributed to the effectiveness of surveillance devices. The law enforcement community and the military as well as other intelligence-gathering agencies have supported this development in order to meet their specific needs. The intent of this section is to provide some broad categories to assist in identifying and discussing the related technology. This listing is not meant to be comprehensive but rather to provide some understanding of the scope and nature of the technology utilized in surveillance activities. Some of the equipment and devices used in surveillance often are used in unrelated fields such as medicine, education, commerce, and exploration. This wide utility for some of the technologies adds another dimension to the difficulty of providing appropriate oversight and controls.

a. *Electronic Eavesdropping.*—Audio surveillance using specialized equipment to intercept or amplify voice transmissions has received considerable attention in both the public and private sector. Its wide use in surveillance and counter-surveillance activities has stimulated the need to control and regulate adequately the utilization of this technology. The reliability and miniaturization of these communication devices have further encouraged their use. Although controlled by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. 2510 et seq.), this equipment continues to be used legitimately as well as illicitly. The Law Enforcement Assistance Administration report, "Electronic Eavesdroppnig Techniques and Equipment," [25] classifies this type of equipment into three broad categories, namely, radiating devices and receivers, nonradiating devices, and tape recorders.

(1) *Radiating Devices and Receivers.*—This equipment consists of miniaturized transmitters that can be concealed and used where unrestricted mobility is needed. Generally these devices are used in a limited time period and are not hardwired that is, the source of power is restricted to batteries. Figure 1, Model Communication System, presents a generalized overview of a communication system using this class of devices.[26]



Transmitter

1. Power supply (usually batteries)
2. Electronic circuitry such as the oscillator, modulator, amplifiers, and filters
3. Antenna

Propagation Medium

1. Atmosphere including all physical obstructions and other radio signals

Receiver

1. Power supply
2. Electronic circuitry such as the local oscillator, speaker, amplifiers and filters
3. Antenna

Figure 1.—Model communication system.

[25] Jones, Raymond Nelson. Electronic eavesdropping techniques and equipment, September 1975. Prepared for the U.S. Department of Justice, Law Enforcement Assistance Administration. [At the head of the title: Law Enforcement Standards Program.] Washington, U.S. Govt. Print. Off., 1976.

[26] Ibid., p. 2.

One aspect that has contributed to the acceptance and wide use of this type of equipment has been automatic volume control. This feature assists in providing more sensitive monitoring of conversations. Another important feature is that a miniaturized transmitter, which may be worn on the body or hidden in a room, can monitor both sides of a telephone conversation. These devices have a shortcoming in that they may be detected by the radiated signal they transmit and can be located visually.[27]

The drop-in telephone transmitter which may be substituted for the carbon microphone usually found in the mouthpiece of a telephone is another one of the radiating devices being used This device requires only a few moments to be installed but it can be detected by measuring current drain while the telephone is in use.[28]

Receivers in these systems are not usually concealed. Therefore, they are not required to be small. These devices are deemed to be satisfactory when they operate with a high degree of sensitivity, frequency control, and some selectivity.

(2) *Nonradiating Devices.*—This group of devices transmits information over hardwire, generally utilizing existing networks such as telephone systems. These wired surveillance systems have some advantages over radiating or broadcasting devices.[29] While most radiating devices' range is measured in feet, the nonradiating system may be viable for miles.[30] Some of the wired surveillance devices' advantages and disadvantages are noted in Figure 2, adapted from the LEAA report.[31]

Advantages and Disadvantages of Wired Surveillance Systems

ADVANTAGES	DISADVANTAGES
1. Unlimited range.	1. Prior access to premises required.
2. Operating time not limited by battery life.	2. Lack of mobility.
3. Not subject to radiated electromagnetic interference.	3. Outlawed in some states, court order required in others to use telephone system.
4. Not detectable by electromagnetic sensors.	4. Installation requires highly skilled people.
5. Personal contact with subject not required.	

FIGURE 2

Telephone taps, which fall into this category, generally use the existing communication network permitting access to all transmissions on these lines. The telephone may also be used to monitor conversations in a room. The infinity transmitter or "harmonic bug" allows transmission of room conversation. These "bugs" are in effect switches that respond to a tone which activates the devices.[32]

Concealed microphones which use wire or in some instances conducting paint are also used to transmit information. Although it is beyond the scope of this paper to permit a discussion of the extensive tech-

[27] Ibid., p. 13.
[28] Ibid., p. 14.
[29] With the advent of satellite and related technologies these limitations may not be as significant.
[30] Ibid., p. 30.
[31] Ibid., p. 34.
[32] Ibid.

nology associated with microphones, it is important to note the diversity and advanced capabilities permitted by this technology.

(3) *Tape Recorders.*—Tape recorders provide a wide range of surveillance techniques. In this category open-reel tape recorders, cassette tape recorders, and telephone recording actuators, permit a wide range of applications.[33] Most of these devices are sold on the open market and are widely used in many applications. The low cost and convenience of these devices make them a common item. Their use in surveillance is recognized and generally understood.

b. *Optical/Imaging Technology.*—The wide diversity of optical devices and related equipment allows only a cursory examination of this complex area. This section briefly touches on some of the optics technology that may be used in surveillance operations. Photographic techniques, including infrared and ultraviolet photography, television systems, telescopic instrumentation, and night vision devices are but a few of the relevant tools in this area. The high level of sensitivity and quality coupled with relatively low cost for some of the equipment has stimulated its use in both the military and civilian sector.

The Swedish Armed Forces Research Institute, at the request of the Swedish Committee for the Protection of Privacy, prepared a study entitled "Invasion of Privacy with Optical and Electro-Optical Means." [34] The report examines some of the optical technical developments that may have a possible impact on the right of privacy. Highlighted are the developments such as miniature cameras, fiber optics, light amplifiers, image converters, thermal image cameras, laser applications and related devices.[35]

(1) *Photographic techniques.*—Miniature cameras and other still-picture cameras have had an extensive role in surveillance operations. In recent years these tools have been enhanced so that there have been some remarkable improvements. The camera (both moving and still) has been greatly improved by coupling with other technologies. For example, non-visible light spectrum sensitive films have added greatly to improving photographic capabilities under special conditions. Other contributions include the increased capability due to better lens development and increased sensitivity.

(2) *Television.*—Two developments in television have greatly enhanced the capability of this tool being used in surveillance. One is the availability and low cost of closed circuit television. This permits an area to be examined with immediate and future playback. The television camera can be used to remotely monitor happenings in a set time period as well as specific transactions. Another development that may provide indirect surveillance is the emergence of cable TV. The use of TV in this mode permits indirect or passive surveillance of an individual's preference or selection of television programs. Some critics fear that in the future this may provide an excellent means of control or oversight of viewing selection by a cable-TV subscriber.

(3) *Night vision devices.*—Night vision devices employ an image intensifier to provide the capability to view objects under low light

[33] Ibid.

[34] Wahren, Patrik. Invasion of privacy with optical and electrooptical means. Prepared for the Research Institute of National Defense, Stockholm, Sweden, Report FOA–2, September 1968. [At the head of the title: NASA Technical Translation NASA TT–16, 862]. Washington, National Aeronautics and Space Administration, 1976.

[35] Ibid., p. 18.

conditions. A night vision device complete with objective lens but without searchlight is generally referred to as a passive night vision device and it is distinct from an active night vision device which has a viewer and search light as an assist. Figure 3 presents a simplified sectional drawing of a viewer.[36]

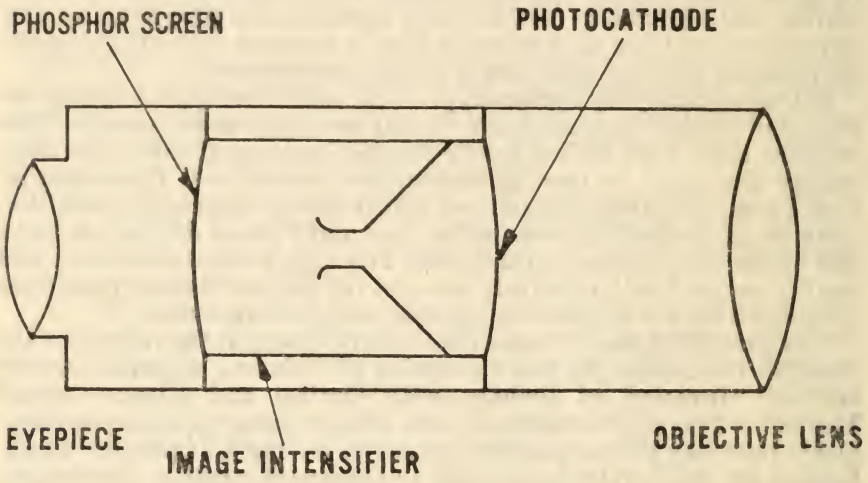


FIGURE 3.—Schematic sectional drawing of a viewer.

c. *Computers and Related Technologies.*—Recent innovations and advances in information technology have contributed to present concerns that these tools and techniques may invade personal privacy and infringe on civil liberties. Computers, unlike some of the other surveillance devices described, have a passive function in surveillance activity. They provide assistance in the record-keepng and data-handling operation and may be used to enhance other surveillance devices. Computers, which have an important role in modern information processing, have the ability to handle vast amounts of data. The proliferation of records, specifically those that contain personally identifiable information, provides the basis for recent concerns. The capability to access files and records from remote locations through communication networks has added to the concerns that the computer may be used to invade personal privacy. The growth of shared data bases (information) and the potential to centralize records have given an additional dimension to the privacy problem.[37]

What is feared is the use of unrelated computerized records and files to assist in developing personal dossiers in order to keep track of an individual's activities. Since records containing social, educational, medical, and financial information on individuals are being computer-

[36] U.S. Department of Justice. Law Enforcement Assistance Administration. National Institute of Law Enforcement and Criminal Justice. NILEC Active night vision devices. A voluntary national standard promulgated by the National Institute of Law Enforcement and Criminal Justice, June 1975 [Washington, 1975], p. 4.

[37] Becker, Louise. Privacy: information technology implications. Issue Brief No. 74–105. [Washington, U.S. Library of Congress. Congressional Research Service, 1976], p. 1.

ized more frequently, it is foreseeable that these may be used to assimilate extensive and multi-faceted dossiers on individuals. Computerized records may provide a viable means of keeping track of individuals and their activities. In addition, computer technology coupled with other technologies may be used to greatly enhance surveillance capabilities.

"File technology," a concept examined in the Senate Select Committee on Government Operations with Respect to Intelligence's study "Intelligence and Technology," and discussed above, illustrates the use of the computerized records in the surveillance process. Significantly, the increased dependency on computers and information systems has stimulated the tendency to consider collecting and maintaining more and more data. The lowered cost and recent technological developments have facilitated access and processing which has contributed to expanded use of file technology.

Although it is generally agreed that computers are an important resource that must be appropriately used to achieve important benefits, it is also understood that there may be a necessity to impose restraints on the collection and dissemination of select information. Included would be establishing better administrative procedures and encouraging the development of appropriate management and product technologies to protect personal privacy and ensure computer security. (For further information, see the memorandum in Chapter III, Section B.3., entitled "Computer and Information Security in the Federal Government: An Overview.")

d. *Sensors.*—Sensors systems basically detect, transmit, and receive alarm signals and in some cases actually activate an alarm. These sensors, generally classified a counter-intrusion sensors, provide an added guard force or observer capability while permitting monitoring of large areas effectively. Many of these systems not only sense but can differentiate regarding the type of intruder or penetrator. Although sensors are passive surveillance devices, they have some interesting potential not fully explored. Coupled with other surveillance devices sensors may provide effective and efficient means to monitor individuals or groups. For example, sensors monitoring an area can be coupled with television cameras so that visual surveillance of an area can be made. There are several types of sensors among which are magnetic, seismic, infrared, pressure, strain, electromagnetic, and acoustical.[38] These are briefly described below:

Magnetic Sensors

Magnetic sensors detect changes in the local geomagnetic field caused by the movement of feromagnetic objects within the sensor's range. The permanent or residual magnetism of an object carried or worn by an intruder distorts the local geomagnetic field. This distortion is detected by the sensor and when the sensor's detection criteria are satisfied, an intrusion alarm is generated.

Seismic Sensors

Seismic sensors detect pressure waves caused by impacts on the earth's surface or by shifting inside the earth. Seismic sensors use a buried geophone to detect the earth-transmitted seismic wave. The geophone is typically emplaced vertically and as such detects seismic waves traveling in the earth's surface plane and within a detection radius around the geophone.

[38] Basic concepts of sensor systems, what commanders should know. Commander's digest, Sept. 20, 1973, p. 4.

Infrared (IR) Sensors

IR sensors detect an intrusion either by the interruption of an IR beam (active IR sensor) or by detecting the difference between an intruder's IR radiation and the background IR radiation (passive IR sensor). The active IR sensor generates a narrow IR beam which impinges on an IR receiver. When an intruder crosses the IR beam, the decrease in IR radiation is sensed by the IR receiver and an alarm is generated.

Strain Sensors

Strain sensors detect the soil stress caused by an intruder's weight. When the detected stress level exceeds a threshold level, an alarm is generated. Generally, strain sensors only detect stress relatively close to the sensor. This limited range and an adjustable minimum stress level requirement can provide good false alarm rejection, especially in areas having background seismic noise.

Electromagnetic Sensors

Active electromagnetic sensors generate a radio frequency (RF) field which is disturbed by an intruder. This disturbance changes the transmitting antenna impedance and causes the transmitted frequency to shift upward and downward as the intruder moves. These frequency shifts are used to determine the presence of an intruder.

Acoustic Sensors

Passive acoustic sensors listen for noises generated by personnel or vehicle intrusion. The noise signal is either processed and compared against detection criteria to determine if an intrusion occurred or a burst of sound is transmitted to a monitoring receiver for operator analysis. Combining the technical challenges of remote sensors with the requirement for low cost, small light sensors capable of being implanted by a variety of methods results in a complex engineering problem with many trade-offs, an almost infinite range of possible solutions, and a requirement for sophisticated techniques stretching the state-of-the-art.[39]

Sensors generally are used in specific areas to prevent unobserved penetration and are considered as counter-intrusion devices. They may be coupled to television cameras or other imaging technologies to provide an immediate identification of the intruder. Primarily developed for and by the military, sensors have also achieved wide acceptance as viable crime counter-measure tools in the private sector.

e. *Other Devices and Techniques.*—Recent technological innovations and specific electronics developments have contributed to the application of a host of new tools and techniques to surveillance. The equipment included in this and the other sections are meant to provide a basic framework for understanding the technological implications in surveillance. It is not meant to be an intensive or comprehensive listing, but rather a base in order to appreciate the role of technology in surveillance activities.

While most of the technology presently available has benign and beneficial uses, there is the potential that it can be used to monitor and even control the lives of individuals. For example, citizens' band radios are being purchased and used by a substantial part of the population. The impact of this equipment on surveillance activity may not be immediately evident. But it is possible that, in some instances, the citizens' band radio has been used to assist law enforcement officers in monitoring and controlling drug traffic and other illicit enterprises.

Another technique that may have implications in surveillance operations is the use of automatic tracking or automatic vehicle location systems. A report of the Law Enforcement Standards Program, "Auto-

[39] Ibid.

matic Vehicle Location Techniques for Law Enforcement Use," [40] describes three categories of systems used to locate moving vehicles, namely—

> Dead reckoning systems: The vehicle carries instruments to measure direction and distance traveled. From these data a computer determines the estimated vehicle position.
>
> Proximity systems [a system of car emitters and sensors]: These systems identify a vehicle when it passes near certain fixed locations. These locations may be equipped with either sensors or emitters for signaling the vehicle, usually by radio.
>
> Radiolocation systems: These systems use the unique characteristics of radio fields themselves to establish vehicle location, as contrasted to use of radio to report vehicle location. They must employ more than one fixed radio treminal in order to operate. Trilateration, triangulation, and navigation systems are in this category.[41]

This technology may have serious implications and may be used in surveillance activities, including the location of police or other types of vehicles. These tracking systems, with some modification and special equipment, can be used to monitor individuals and documents.

Utilizing a machine-readable magnetic strip, credit cards and other documents make use of modern technology to convey special information or characteristics. Some proposals have been made and are being considered to use this technology to process passport information. There has been some discussion on the instituting of a machine readable passport with select information that would not be visible, but could be electronically read. This system might include a magnetic strip to permit electronic readers to scan passports so that travelers could be processed more efficiently while noting specific characteristics through selective coding.[42] This is another technology that potentially may be used to oversee the activities of individuals or groups.

Polygraph testing, as an overt surveillance device, remains controversial yet highly acceptable in many quarters and has acquired expanded utility in various aspects of surveillance. Originally developed in the 1920's, yet still undergoing refinements and modifications, the polygraph test measures stress on specific bodily changes, such as blood pressure, respiratory patterns, and other physiological reactions. [See Chapter III, Section B. U.S. House Government Operations. "The Use of Polygraphs and Similar Devices by Federal Agencies."] In examining the problems of privacy and the use of polygraphs in employment, the Staff of the Senate Judiciary Subcommittee on Constitutional Rights Commented on the reliability of the polygraph:

> The theory behind the polygraph procedure and its results involves physiological responses purportedly related to the act of lying. It is professed that lying causes conflicts to arise within the individual subject. The conflict produces fear and anxiety which, in turn, produce physiological changes which the polygraph devices can measure and record. Thus, the assumption underlying the polygraph test is that a uniform relationship exists between an act of deception, certain specific emotions, and various bodily changes.[43] The report observed that—Though

---

[40] U.S. Department of Justice. Law Enforcement Assistance Administration. National Institute of Law Enforcement and Criminal Justice. Automatic vehicle location techniques for law enforcement use. Washington, 1974. [At head of title—Law Enforcement Standards Program].

[41] Ibid., pp. 1–2.

[42] Wells, Benjamin. The age of the electronic passport. Washington Post, July 22, 1976.

[43] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Privacy, polygraphs and employment. 93d Congress, 2d sess. Washington, U.S. Govt. Print. Off., 1974, p. 5.

studies and experiments to assess the polygraph's effectiveness have been done, even when interpreted favorably, their results seem far from convincing of the polygraph's reliability.[44]

Another developing technology is the "voice stress analyzer," a device that can interpret and measure emotional conflicts by voice modulation. Today, a voice stress analyzer, no larger than a book, is available at a relatively low price. The low cost and the possibility of further miniaturization may lead to widespread use in both the government and the private sector. Unlike the traditional polygraph systems, the subject in this instance is rarely aware that he is being tested or examined. Although the validity of such testing may be questionable, the accessibility and general appeal may stimulate its further usage in the future. It does not require a great deal of imagination to visualize how such a device may be used in employment interviews, educational counseling, and criminal justice operations, as well as clandestine surveillance operations.

A recent advertisement for a wristwatch clock/calculator raises the possibility of a technological advancement thought to be next to impossible less than a decade ago. This device utilizes the electronic digital face of the watch to give results of the time as well as calculations. It is not difficult to imagine combining other distinct but potentially related technologies in order to obtain greater capability. For example, it is conceivable that a voice stress analyzer could be developed that would be as small as a wristwatch.

Innovations in microwave technology have progressed to permit extensive communications networks as well as the development of interception devices. Most recently the potential hazards associated with radiation from these electronic techniques have been brought to public attention. A *New York Times* article of February 9, 1976, commented on the health hazards from microwave emanations on American Embassy personnel in Moscow.[45] Reportedly, the staff of the American Embassy in Moscow was briefed on the radiation implications. The article went on to note that—

> The disclosure led to some confusion here as to whether the Russians were using radiation directly for eavesdropping. This was discounted by one source who understood that the radio waves were operating and energizing the existing electronic bugs, though a more modern variation could not be ruled out. Allegations were made in Washington in 1972 that the Russians were beaming microwaves at the embassy during the 1960's but this is the first time in more recent years that the issue has risen.[46]

The continuing concern with microwave use for surveillance is also paralleled by the developments in microwave interception of messages, as outlined in the report by the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities. (See text in Chapter V, Section A, "Review of the Technology.")

Message interception by microwave and other advanced technologies, such as laser, presents an important development in surveillance technology. These innovations permit the interception of messages without visible communication linkages. Although they might be detectable

---

[44] Ibid, p. 6.
[45] Wren, Christopher S. Bugging in Moscow causes health scare. New York times. Feb. 9, 1976, p. C4.
[46] Ibid.

through emission monitoring and other techniques, they remain a new and undetermined force in surveillance operations.[46a]

(4) *Perspectives and Prospects.*—The concern in both the public and private sector is with the growing involvement of surveillance technology in everyday life. It has been predicted that during the next few decades progress and developments in both space and military technology will have a further significant and direct impact on surveillance tools and techniques. Some of these recent developments are discussed in an article by Ivan Bekey and Harris Mayer of the Aerospace Corporation, "1980–2000, Raising Our Sights for Advanced Space Systems." [47]

This article is based on an in-depth study by the Aerospace Corporation for the National Aeronautics and Space Administration (NASA). The study outlines some of the "space-systems concept with potential utility in national security and civilian space areas." [48] Although the article does not purport to evaluate or suggest the economics of the technological concepts nor all relevant implications for society, it does outline "reasonable extrapolations of today's technology" to future developments.[49]

Highlighted are some of the advanced microwave applications and optical systems, with some emphasis on communication satellite which would encourage the development and utilization of personal wrist radio and navigation sets, intrusion detection, electronic mail transmission, data sharing, border surveillance, etc. Some of the applications of aerospace-generated technology are listed in Figure 4. [50]

PERSONAL

Personal Communications Wrist Radio.
Emergency Rescue Wrist Beacon.
Personal Navigation Wrist Set.
Voting/Polling Wrist Set.

CIVIC

Disaster Communications Wrist Radio.
All-Aircraft Traffic Control.
Urban/Police Wrist Radio.
Car Speed-Limit Control.

INDUSTRIAL

Burglar Alarm/Intrusion Detection.
Vehicle/Package Locator.
3D Holographic Teleconferencing.
Advanced TV Broadcast.
Advanced Resources/Pollution Observation.

INTERNATIONAL

Nation-Nation "Hot Lines."
Multinational Air Traffic Control Radar.

[46a] Various surfaces in a room, e.g. window panes, will resonate in response to acoustical energy of conversations. A small inconspicous reflector directed on such a surface (acoustical disk or acoustical reflector) will modulate a laser beam. A photo cell, receiving the reflected beam will convert the signal back into sound, thus revealing the conversation. The interception of messages can also come from the monitoring of electronic emissions generated by electrical typewriters, computers, and related equipment presents a problem in many environments.

[47] Bekey, Ivan and Harris Mayer. 1980–2000, raising our sights for advanced space systems. Astronautics and aeronautics, July–August 1976, pp. 34–63.

[48] Ibid., p. 35.

[49] Ibid.

[50] Ibid., p. 36.

Small Terminal Intelsat Network.
Earth Resources Data Sharing.
Energy Distribution Relay.
U.N. Truce Observation Satellite.

SCIENTIFIC

Astronomical Super Telescope.
Interplanetary TV Link.
Atmospheric Temperature Profile Sounder.
Ocean Resources and Dynamics Sensor.
Water Level and Fault Movement Indicator.

GOVERNMENT

Communications

Voting/Polling Wrist Set.
Electronic Mail Transmission.
Border Surveillance.
Nuclear Materials Locator.
Library Data Sharing.

Observation

High Resolution Resources/Pollution Observatory.
Water Level and Fault Movement Indicator.
Atmospheric Temperature Profile Sounder.
Forest Fire Detection.
Ocean Resources Location.

Support

Passive Coastal Anti-Collision Radar.
Night Illuminator.
Energy Delivery and Distribution (5 concepts).
Energy Consumption Monitor.
Aircraft Laser Bean Powering.
Nuclear Waste Disposal.

FIGURE 4.—*Applications*

The implications for surveillance technology developments are clear in a number of the applications listed. When coupled with other developments, it becomes evident that future technological advances will provide additional surveillance capabilities.

It should be understood that the use of technologies in surveillance applications is not dependent on special or unique developments, but rather on the applicability and utility inherent in selective devices and equipment. Much of the technology being used has benign aspects and in some cases the utility of the device in non-surveillance operations will determine its total development and availability. Selected technological developments, in all probability, will remain controversial while they continue to provide society with benefits and specific advantages. The capability to monitor and measure individuals and the potential to invade personal privacy generally resides in the application of the technology. The administrative practices and procedures remain a critical element in the management and use of the technology.

Continued modifications in instrumentation coupled with lowered cost will greatly contribute to the use of technological innovations in surveillance. There are some other developments that may increase surveillance capabilities. One of the areas which remains exceedingly controversial is the use of chemical agents and other mind-probing mechanisms that may be used to enhance surveillance capabilities.

Certain technological developments will in all probability continue to provide a basis for concern because of the potential use in surveillance activities. While total assessment of surveillance innovations must be done in light of a society's values and needs, the specific applications of technology must be conducted within the appropriate administrative and legal framework.

C. Congressional Action

Congressional awareness and involvement regarding surveillance technology has taken a number of forms, spanned a wide variety of issues associated with the topic, and included a substantial number of committees in the process. This section briefly examines that recent involvement and the role of the Senate Subcommittee on Constitutional Rights, both of which are more comprehensively and thoroughly reviewed in Chapter III, "Congressional Action and Reaction."

Congressional involvement has been manifested in several forms—congressional structuring, enactment of legislation, and oversight. Indirectly, the restructuring of congressional jurisdiction with respect to intelligence is related to revelations and growing concerns with surveillance technology practices and abuses and improprieties of surveillance authorities held by certain Federal agencies. The prominent intelligence community investigations of the 94th Congress, conducted by the specially created House and Senate select committees on intelligence, are the most direct example of that concern. The broad mandate and complementary jurisdiction of both these temporary committees permitted them to focus on elements of surveillance technology policy and implications—among others, the domestic surveillance operations of intelligence units of DEA (Drug Enforcement Administration), FBI, the U.S. Customs Service, and CIA;[51] the role of the National Security Agency and its monitoring activities regarding U.S. citizens on "watch lists" on behalf of domestic agencies, such as the Secret Service and the FBI;[52] and mail openings, electronic surveillance, and access to and use of confidential records and files maintained by various agencies.[53]

The creation of the permanent Senate Select Committee on Intelligence (S. Res. 400, approved May 19, 1976) is another indication of congressional restructuring which has an impact on issues related to surveillance technology. The extensive legislative authority and jurisdiction of the new committee, including all major intelligence agencies, their organizations, and activities, are complemented by its comprehensive oversight mandate:

> To provide vigilant oversight over the intelligence activities of the United States to assure that such activities are in conformity with the Constitution and laws of the United States. (Sec. 1, S. Res. 400)

---

[51] U.S. Congress. House. Select Committee on Intelligence. U.S. intelligence agencies and activities; domestic intelligence programs. Hearings, 94th Congress, 1st session Oct. 9–Dec. 10, 1975.

[52] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. The National Security Agency and Fourth Amendment rights. Hearings. 94th Congress, 1st session, Oct. 29 and Nov. 6, 1975.

[53] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Internal Revenue Service. Hearings, 94th Congress, 1st session, Oct. 2, 1975; ——. Mail opening. Hearings, 94th Congress, 1st session, Oct. 21, 22, and 24, 1975; ——. Federal Bureau of Investigation. Hearings, 94th Congress, 1st session, Nov. 18–Dec. 11, 1975.

A series of legislative enactments since the late 1960's have marked a growing congressional awareness of the need for more explicit requirements and controls on the use of certain surveillance operations, technologies, and applications. The principal legislation includes—

(1) Omnibus Crime Control and Safe Streets Act of 1968 (Public Law 90–351);

(2) Fair Credit Reporting Act of 1970 (Public Law 91–508);

(3) Crime Control Act of 1973 (Public Law 93–83);

(4) Family Educational Rights and Privacy Act of 1974 (Public Law 93–380); and

(5) Privacy Act of 1974 (Public Law 93–579).

These statutes provided for prohibitions on the interception and disclosure of wire or oral communications by private parties or government officials without court authorization (Public Law 90–351); regulations for consumer reports and investigative consumer reports on both collectors and users (Public Law 91–508); limitations on the use of criminal history files and subject access and corrective procedures for such files (Public Law 93–83); regulation of school records of educational institutions receiving Federal funds and subject access to such records (Public Law 93–380); and subject access to personal records held by Federal agencies, limitations on the disclosure of information held in those records, restrictions on the use of Social Security numbers, and the creation of the Privacy Protection Study Commission (Public Law 93–579).

Present legislative interest in the Senate centers on the Foreign Intelligence Surveillance Act of 1976 (S. 3197), amended versions of which have been approved by the Committees on the Judiciary and on Intelligence. The bill incorporates provisions dealing with electronic surveillance for national security purposes, which are presently exempted from statutory controls. But the bill has been criticized for concentrating too much authority in a proposed judicial tribunal, lacking adequate defintions of critical concepts, and failing to specify relevant surveillance devices.[54]

On the House side, legislative interest includes a series of bills before the Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice. The proposals deal with new standards for surveillance practices and procedures, subject consent in oral communications interception, court authorizations for communications interceptions and inspection of certain records, and prohibitions on military surveillance of civilians and on the illegal surveillance of citizens by civil officers of the United States.[55]

Congressional oversight of surveillance and surveillance technology has crossed a variety of subject matter jurisdictions and topic areas. Oversight hearings in the 93d and 94th Congresses have included the major subjects of surveillance technology per se, electronic surveillance for national security purposes, Government surveillance of Federal employees, criminal justice information systems, computer security and abuses, and use of polygraphs in the public and private

[54] U.S. Congress. Senate. Committee on the Judiciary. Foreign Intelligence Surveillance Act of 1976. Report together with additional and minority views (to accompany S. 3197). 94th Congress, 2d session, July 15, 1976.

[55] U.S. Congress. House. Committee on the Judiciary. Subcommittee on Courts, Civil Liberties, and the Administration of Justice. Hearings, 94th Congress, 1st session, Feb. 6–Sept. 8, 1975.

sectors, among others. The use of surveillance technologies by a multiplicity and variety of Federal agencies suggests that congressional oversight will be correspondingly dispersed among committees. In addition to the select committees on intelligence in both chambers, other committees which now conduct public inquiries have included the following—the Committees on Government Operations and Judiciary in both chambers, the Committee on Finance in the Senate, the Committee on Ways and Means in the House, and the Joint Committee on Internal Revenue Taxation.

Congressional activity in the area of surveillance technology is not limited to the present but extends back to at least 1934 and the passage of the Federal Communications Act of that year. One recent congressional inquiry into electronic surveillance noted that "between 1934 and 1967 at least 16 sets of congressional hearings on wiretapping were held." [56]

The Judiciary Committees of both the House and Senate have been principals in the examination of various surveillance technologies and have had a relatively lengthy history of involvement. Their basic responsibilities include that subject matter through several jurisdictional ingredients—among others, judicial proceedings, civil and criminal, generally (e.g., evidence admissibility related to electronic surveillance); Federal courts and judges (e.g., proposed judicial tribunal in the Foreign Intelligence Surveillance Act of 1976 and court authorization of wiretaps); revision and codification of the statutes of the United States (e.g., Title 18 of the United States Code relating to interception of oral communications); and civil liberties (e.g., invasion of privacy, "chilling effect" on constitutional rights of free speech, free press, peaceable assembly through various surveillance technology utilizations).

The Senate Committee on the Judiciary Subcommittee on Constitutional Rights, which commissioned this study, has an extensive heritage of inquiry and examination of surveillance technology and its impact on civil liberties and the right of privacy. That heritage was summarized in a 1974 committee publication:

> Among the first activities of the Constitutional Rights Subcommittee after its creation at the beginning of the Eighty-fourth Congress, were extensive hearings on "Security and Constitutional Rights." These 1955 hearings which focused on government security-loyalty programs were followed in the Eighty-fifth Congress by subcommittee hearings on "Wiretapping, Eavesdropping and the Bill of Rights" and "Freedom of Information and Secrecy in Government." During the Eighty-sixth Congress the subcommittee renewed hearings on all three of these privacy-related subjects.
>
> Soon after Senator Sam J. Ervin, Jr., became chairman in 1961, the Constitutional Rights Subcommittee began to concentrate on governmental infringements of individual privacy. The subcommittee's work on questions of employee procedural rights led directly to a consideration of the kinds of information that the Federal government as an employer finds pertinent in actions involving its employees. The subcommittee found ever-increasing demands by the Federal government to learn about its employees, applicants for Federal employment, and their families, activities and associations. The subcommittee soon discovered that these efforts were not limited to government employees. There was widespread use of psychological testing and intrusive questionnaires seeking to learn all about citizens who were not employees or prospective employees of government.

---

[56] U.S. Congress. House. Committee on the Judiciary. Subcommittee on Courts, Civil Liberties, and the Administration of Justice. Wiretapping and electronic surveillance. Hearings, 93d Congress, 2d session, April 24, 26, and 29, 1974, p. 2.

These investigations resulted in a series of bills and hearings in the mid-1960's. Chief among these were hearings on "Psychological Tests and Constitutional Rights" in 1965; "Privacy and the Rights of Federal Employees" in 1966; and "Privacy, the Census, and Federal Questionnaires" in 1969. These hearings served to increase general interest in privacy. The subcommittee's initial privacy proposal, the Government Employees Privacy bill, passed the Senate numerous times in the years since the 1966 hearings and met little Senate opposition. However, it died in the House each time. Other privacy bills did not advance so far.

As these privacy-related studies were conducted, it became evident that each was merely part of a more general problem of individual privacy versus government accumulation of data. It also became apparent with the debate on the proposed National Data Center that the advent of computers introduced a new and ultimately a very threatening element into the privacy problem. More and more citizens brought to the subcommittee's attention the fact that the programs intruding on privacy and other individual rights were utilizing computers to assist the government in its activities. Thousands of complaints about the use of computers in these programs urged further subcommittee investigation of the impact of computers on individual privacy. . . .

The controversy over the National Data Center introduced Congress to the computer, but it was the increasing concern on the part of individual citizens that sparked the subcommittee's particular interest. From that point the subcommittee became more and more concerned not only about data collection in itself, but also about the consequences that would follow as the computer was employed to store and interrelate government data. This focus eventually resulted in the 1971 hearings on "Federal Data Banks, Computers, and the Bill of Rights." These hearings explored for the first time the use of computers in data collection about citizens.[57]

Congressional involvement in regard to surveillance technology although extensive, has been sporadic and has lacked a comprehensive strategy. The most recent hearings on surveillance technology, held jointly by the Senate Judiciary Subcommittee on Constitutional Rights and the Commerce Special Subcommittee on Science, Technology, and Commerce, provide the first overview of the topic and potential possible ramifications.[58] Senator John Tunney, chairman of both Subcommittees, introduced the hearings, citing their necessity and purposes:

The need for such hearings is overwhelming. Technological developments are arriving so rapidly and are changing the nature of our society so fundamentally that we are in danger of losing the capacity to shape our own destiny.

This danger is particularly ominous when the new technology is designed for surveillance purposes, for in this case the tight relationship between technology and power is most obvious. Control over the technology of surveillance conveys effective control over our privacy, our freedom, and our dignity—in short, control over the most meaningful aspects of our lives as free human beings.

Yet, surveillance technology, despite its significance in terms of public policy-making, has remained largely unscrutinized. James Reston of the New York Times discussed this problem during the Watergate crisis of 1973:

"What has happened here over the last postwar generation is that the scientific capacity to use the arts of wartime espionage on private citizens has greatly expanded while the political capacity to control all this has actually declined."

There is a suggestion in Reston's statement that we are internalizing the cold war—turning upon ourselves its attitudes, techniques, and technologies. If that is true, then the White House enemies list was not an aberration, but a brief reflection of reality. And certainly the revelations of the recent past reinforce this belief by demonstrating the inherent danger of concentrating extraordinary

[57] U.S. Congress. Senate. Committee on the Judiciary. Subcommitte on Constitutional Rights. Federal data banks and constitutional rights, op. cit., pp. XXXIII–XXXIV.

[58] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Committee on Commerce. Special Subcommittee on Science, Technology, and Commerce. Surveillance technology. Joint hearings, 94th Congress, 1st session. June 23, Sept. 9 and 10, 1975.

powers behind a rigid curtain of secrecy. Continued ignorance of surveillance technology—its size and structure as a separate industry, the justifications for its growth, its impact on society—could prove to be an Orwellian catastrophe for our privacy and our freedoms.[59]

This particular examination and compendium of materials on "Surveillance Technology Policy and Implications" is a supplement to those hearings and continued congressional interest.

D. Policies and Implications of Surveillance Technology

In examining the policies and derivative implications of surveillance technology, this section confines itself to the Federal Government and its contribution to subnational governments through technology transfer programs and certain assistance provided by the Law Enforcement Assistance Administration (LEAA) of the Department of Justice. This section does not review practices or procedures utilized in the private sector nor does it focus directly on State and local government programs in surveillance technology.

The ability to provide an examination of even the Federal Government policies and programs is extremely circumscribed for several critical reasons. Much of Government surveillance, use of surveillance technology, and development and research into various related devices and technologies is secret and precluded from public view. Moreover, possible congressional inquiries into these topics or reviews by congressional support agencies, such as the General Accounting Office (GAO), might themselves be held in executive session, and therefore, are unavailable for public consumption or are sometimes even proscribed. An illustration of these restrictions involves some of the responsibilities and authorities of GAO regarding two intelligence agencies which have conducted surveillance on American citizens—the National Security Agency (NSA) within the Department of Defense and the Central Intelligence Agency (CIA). GAO conducts on-site audits of NSA. But because of the sensitive and confidential nature of NSA operations, the results of the studies are not publicly available, in compliance with Public Law 86–36 (73 Stat. 63, passed on May 29, 1959), which forbids disclosure of any information regarding NSA activities. The CIA, on the other hand, is exempt from GAO audits, other than by the Agency's own request, and has not undergone a comprehensive GAO audit since 1961.[60]

This section does not purport to review all the policies and implications of surveillance technology as employed by the Federal Government. That massive undertaking would require long-term, comprehensive examinations utilizing the full resources available to the Congress, including the support agencies, such as the General Accounting Office, the Office of Technology Assessment, the Congressional Research Service, and the Congressional Budget Office. This section can, however, provide a preliminary framework within which to assess the

[59] Ibid., pp. 1–2.

[60] For a more extensive review of the restrictions on congressional and GAO investigative authorities regarding intelligence agencies, see Library of Congress. Congressional Research Service. Congressional oversight of intelligence: status and recommendations. Multilith No. 76–54 G, prepared by Frederick M. Kaiser, March 11, 1976, pp. 10–32. (A copy of the multilith is included in Chapter III, Section B.3, Congressional Research Service Reports.)

policies and implications, illustrate and describe some of the ingredients, and suggest some questions and problems regarding such policies. The section is divided into two main categories—policies and implications—and elaboration of both is found in Chapter V, Section B, "Civil Liberties Issues and Policy Implications," among other chapters identified in the text.

1. Surveillance Technology Policies

A preliminary inquiry into surveillance technology policies reveals that there is no comprehensive, integrated Federal policy in this area. The variety, diversity, and multiplicity of agencies conducting surveillance and employing appropriate technology combined with transformations in its utilization over time apparently preclude a consistent, over-arching policy associated with surveillance technology. The Federal agencies and programs utilizing surveillance technology have varied responsibilities, duties, and authorities, which produce, in turn, different approaches to and employment of that technology. Moreover, these functions of the agencies have been transformed during the recent history of the United States as the Federal Government has acquired additional responsibilities in the areas of law enforcement, intelligence production, and national security.[61] The different institutional heritages of the various agencies and their independence in terms of organization, authority, and procedures also contribute to the absence of a standardized Federal policy in this area.

In order to analyze the multiplicity of resultant policies associated with surveillance technology, two principal ingredients of policy will be examined—the scope and magnitude of surveillance technology development and utilization by the Federal Government, and the authorities and standards associated with the generation and application of surveillance technology. Again a disclaimer is essential. This particular study is but a preliminary examination, intended to develop a framework for further analysis, to raise prominent issues, and provide some description. It is impossible at this point to provide a comprehensive or definitive description and analysis.

a. *Scope and magnitude.*—Federal Government development and utilization of surveillance technology, as defined in this report, have expanded beyond a modest state at the commencement of this century to a present capacity whose scope and magnitude defy reliable measurement. Certain indicators, however, suggest that the extent of Federal support and utilization of surveillance technology is varied and widespread, if not commonplace, and, in some instances, extremely sophisticated and intensive. An examination of the scope and magni-

[61] Descriptions of the agency transformations and acquisitions of authority are available in the following sources: U.S. Congress. Senate. Select Committee to Study Government Operations with Respect to Intelligence Activities. Final Report, op. cit. Book I: Foreign and military intelligence, pp. 15–277; Book II: Intelligence activities and the rights of Americans, pp. 30–137; Book IV: Supplementary detailed staff reports on foreign and military intelligence, pp. 1–109; and Book VI: Supplementary reports on intelligence activities, pp. 1–293. Frank Donner. The theory and practice of American political intelligence. New York review of books, April 22, 1971. Vern Countryman. History of the FBI. In Pat Watters and Stephen Gillers (eds.). Investigating the FBI. Garden City, New York. Doubleday, 1973. Lyman Kirkpatrick. The US intelligence community: foreign policy and domestic activities. New York. Hill and Wang, 1973. President's Commission on CIA Activities within the United States. Report. Washington, D.C. U.S. Govt. Print. Off. 1975. Harry Howe Ransom. The intelligence establishment. Cambridge, Mass. Harvard University press. 1970.

tude of Federal involvement focuses on four elements—(1) direct utilization and development, including intelligence and law enforcement operations, (2) technical assistance and grant support, (3) technology transfer, and (4) training programs.

(1) *Direct utilization and development.*—A review of the Federal agencies which have the capacity and authority to employ and support surveillance technology reveals an expanding network, composed of a variety and diversity of units. The principal institutional ingredients are the intelligence agencies and the criminal justice/law enforcement entities but they are not the exclusive users of surveliance technology. Other agencies, such as the Federal Communications Commission,[62] have demonstrated such a facility.

Recent congressional and executive investigations of the intelligence community, prompted by the exposure of relevant agency abuses and unethical practices, have helped to develop an awareness of the scope of intelligence operations and activities in the Federal Government. The following chart lists the units of departments and agencies which have been reported to conduct intelligence and, therefore, utilize surveillance technology. The distinction between major and minor units is based upon their seeming contribution to national intelligence production and/or the primary nature of the intelligence function.[63]

MAJOR INTELLIGENCE UNITS

DEPARTMENT OR AGENCY AND SUBDIVISION (IF RELEVANT)

Central Intelligence Agency (CIA).
Director of Central Intelligence.
Department of Defense (DOD)—
- Air Force Assistant Chief of Staff, Intelligence.
- Army G–2, Assistant Chief of Staff, Intelligence.
- Navy, Marine Corps G–2.
- Navy, Naval Intelligence Command.
- Defense Intelligence Agency (DIA).
- National Security Agency (NSA).

Department of Justice—Federal Bureau of Investigation, Intelligence Division.
Department of the Treasury—Office of National Security.
Department of State—Bureau of Intelligence and Research.

---

[62] A congressional hearing revealed that in 1970 the FCC monitored the telephone conversations of some of its employees surreptitiously and without the required court order. U.S. Congress. House. Committee on Interstate and Foreign Commerce. Special Subcommittee on Investigations. FCC monitoring of employees' telephones. Hearings, 92d Congress, 2d session, March 28 and May 16, 1972.

[63] The prior dichotomy between foreign vis-a-vis domestic intelligence units appears artificial and has proven misleading. Agencies throught to be limited to foreign intelligence operations have embarked on domestic operations, as demonstrated in the recent investigations of CIA surveillance and infiltration of domestic organizations and the NSA assistance to the domestic security responsibilities of the Secret Service (e.g., Presidential protection). Moreover, certain "domestic" intelligence units have "foreign" intelligence by-products. This is especially true of the FBI, which is a member agency of the United States Intelligence Board (USIB), the coordinating unit for national intelligence efforts.

Inter alia. Frank Donner. The theory and practice of American political intelligence. New York Review of books. April 22, 1971; Jim Hougan. A surfeit of spies. Harper's magazine, vol. 249. Nov. 1974; Lyman Kirkpatrick. The U.S. intelligence community: foreign policy and domestic activities. New York. McGraw Hill. 1973; Harry Howe Ransom. The intelligence establishment. Cambridge, Mass. Harvard university press. 1970; U.S. Congress. House. Select Committee on Intelligence. U.S. intelligence agencies and activities: domestic intelligence programs. Hearings, 94th Congress, 1st session. Oct. 9 . . . Dec. 10, 1975 (Part 3); U.S. Congress. Senate. Select Committee to Study Government Operations with respect to Intelligence Activities. Book VI, op. cit., pp. 132–293.

MINOR INTELLIGENCE UNITS

Civil Service Commission—Bureau of Personnel Investigations.
Energy Research and Development Administration (ERDA)—Division of International Security Affairs.
Department of Defense—Defense Investigative Service.
Department of Justice—
Criminal Division.
Drug Enforcement Administration (DEA).
Immigration and Naturalization Service.
Department of State—Passport Office, Bureau of Security and Consular Affairs.
Department of Transportation—U.S. Coast Guard.
Department of the Treasury—
Bureau of Alcohol, Tobacco, and Firearms
Internal Revenue Service
Secret Service
U.S. Customs Service
U.S. Postal Service—Inspection Service (formerly Intelligence Division).

Several illustrations highlight the scope and diversity of Federal utilization and development of surveillance technology as related to intelligence production. The National Security Agency (NSA), created in 1952 by a still-classified Presidential order, is a separate agency within the Department of Defense. The NSA Director has four responsibilities:

Prescribing certain security principles, doctrines, and procedures for the U.S. Government;
Organizing, operating, and managing certain activities and facilities for the production of foreign intelligence information;
Organizing and coordinating the research and engineering activities of the U.S. Government which are in support of the Agency's assigned functions; and
Regulating certain communications in support of Agency missions.[64]

These responsibilities and derivative sophisticated surveillance apparatuses of NSA contribute to requests to assist other Federal entities in compiling information on individuals on "watch lists." [65] That capability of the Agency and its implications were summarized by Senator Frank Church, Chairman of the investigating committee:

We have a particular obligation to examine the NSA, in light of its tremendous potential for abuse. It has the capacity to monitor the private communications of American citizens without the use of a "bug" or "tap." The interception of international communications signals sent through the air is the job of NSA; and, thanks to modern technological developments, it does its job well. The danger lies in the ability of the NSA to turn its awesome technology against domestic communications.[66]

In testimony before the Senate select committee on intelligence, General Lew Allen, Director of NSA, related the genesis of the "watch list" activities:

The activity in question is one in which U.S. names were used systematically as a basis for selecting messages, including some between U.S. citizens, when one of the communicants was at a foreign location.

---

[64] U.S. Government Manual, 1975–1976, p. 216.
[65] U.S. Congress, Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, The National Security Agency and Fourth Amendment Rights, Hearings, 94th Congress, 1st session, Oct. 29, and Nov. 6, 1975.
[66] Ibid., p. 2.

The origin of such activity is unclear. During the early sixties, requesting agencies had asked the NSA to look for reflections in international communications of certain U.S. citizens traveling to Cuba. Beginning in 1967, requesting agencies provided names of persons and organizations, some of whom were U.S. citizens, to the NSA in an effort to obtain information which was available in foreign communications as a by-product of our normal foreign intelligence mission.

The purpose of the lists varied, but all possessed a common thread in which the NSA was requested to review information available through our usual intercept sources. The initial purpose was to help determine the existence of foreign influence on specified activities of interest to agencies of the U.S. Government, with emphasis then on Presidential protection and on civil disturbances occurring throughout the Nation.

Later, because of other developments, such as widespread national concern over such criminal activity as drug trafficking and acts of terrorism, both domestice and international, the emphasis came to include these areas. Thus, during this period, 1967–73, requirements for which lists were developed in four basic areas: international drug trafficking; Presidential protection; acts of terrorism; and possible foreign support or influence on civil disturbances.[67]

NSA "watch list" surveillance capability was made available to several prominent intelligence/law enforcement agencies for their domestic responsibilities, including . . .

Secret Service and its protective responsibilities (180 United States citizens on its "watch list");

The Bureau of Narotics and Dangerous Drugs (later to become the Drug Enforcement Administration) and its investigations of illicit drug trafficking (a "watch list" of 450 U.S. citizens and groups as well as 3,000 foreign individuals);

The Federal Bureau of Investigation and its investigation of foreign agents and their support of certain United States groups and individuals active in civil disturbances (a "watch list" of approximately 1,000 U.S. citizens and groups as well as 3,000 foreign individuals);

The Defense Intelligence Agency and its interest in foreign involvement in U.S. anti-war activity (a "watch list" of 20 U.S. citizens).[68]

Summary tabulations of "watch lists" and the subsequent NSA reports were provided by the Director of NSA to the Senate Select committee on intelligence:

Between 1967 and 1973 there was a cumulative total of about 450 U.S. names on the narcotics list, and about 1,200 U.S. names on all other lists combined. What that amounted to was that at the height of the watch list activity, there were about 800 U.S. names on the watch list and about one-third of these 800 were from the narcotics list.

We estimate that over this 6-year period, 1967–1973, about 2,000 reports were issued by the NSA on international narcotics trafficking, and about 1,900 reports were issued covering the three areas of terrorism, Executive protection and foreign influence over U.S. groups. This would average about two reports per day. These reports included some messages between U.S. citizens with one foreign communicant, but over 90 percent had at least one foreign communicant and all messages had at least one foreign terminal. Using agencies did periodically review, and were asked by the NSA to review, their watch lists to insure inappropriate or unnecessary entries were promptly removed.[69]

Other examples of intelligence agency application of surveillance technology include CIA mail-opening and mail-cover programs, domestic bugging and wiretapping by the Agency, and planned overhearing of conversations of American citizens abroad.[70] Even when unintentional, such employment of technology has serious conse-

[67] Ibid., pp. 10–11.
[68] Ibid., pp. 11–12.
[69] Ibid., p. 12.
[70] U.S. Commission on CIA Activities within the United States. Report to the President. Washington, D.C. U.S. Govt. Print. Off. 1975, pp. 30–31.

quences for individual rights, and represents a potential for abuse. An indication involves the CIA testing of some monitoring equipment, as reported by the President's Commission on CIA Activities within the United States:

> In the process of testing monitoring equipment for use overseas, the CIA has overheard conversations between Americans. The names of the speakers were not identified; the contents of the conversations were not disseminated. All recordings were destroyed when testing was concluded. Such testing should not be directed against unsuspecting persons in the United States. Most of the testing undertaken by the Agency could easily have been performed using only Agency personnel and with the full knowledge of those whose conversations were being recorded. This is the present Agency practice.[71]

Central Intelligence Agency use and generation of surveillance technology exists in its four directorates—Operations, Science and Technology, Intelligence, and Administration. The following chart, prepared by the Defense Intelligence School/Defense Intelligence Agency, provides a description of the Agency directorates and their responsibilities.

CENTRAL INTELLIGENCE AGENCY DIRECTORATES [1]

Deputy Director for Operations	Deputy Director for Science and Technology	Deputy Director for Intelligence	Deputy Director for Administration
Includes geographic area divisions, plans staff, operations staff, services staff, etc.	Includes office of ELINT, technical services, scientific intelligence, research and development, and office of development and engineering, etc.	Includes offices of current and basic intelligence, the operations center, offices of political, economic, and strategic research, library facilities, and imagery analysis.	Includes offices of personnel, training, security, finance, computer support, logistics, communications, etc.
In charge of foreign espionage and counterespionage operations, collecting covert positive and counterintelligence information through agents and informants overseas. This division overtly collects information from U.S. citizens about foreign countries.	In charge of technical intelligence. It provides assessments of foreign advances in science, technology and weaponry.	Responsible for the assembly, analysis, and evaluation of information from all sources. Produces intelligence reports.	In charge of all administrative activities for the agency. It is also responsible for devising the special communication codes used by CIA.

[1] Source: DOD Defense Intelligence School/Defense Intelligence Agency.

The criminal justice/law enforcement segment of the Federal Government represents a second prolific source of surveillance technology utilization and development. In addition to the substantial number of police in investigative agencies, this segment includes other related elements, such as the Law Enforcement Assistance Administration, which support the development and expansion of surveillance technology.

A 1975 survey by the Washington Regional Office of the General Accounting Office itemized eighty Federal units performing police or investigative activities. These units exist among eleven executive departments, nineteen independent agencies, the Congress, and the Supreme Court.[72] While there is some overlap with the intelligence units, it is not complete. The following chart lists the Federal law enforcement agencies included in the GAO report.[73]

---

[71] Ibid, p. 37.

[72] U.S. Congress. Senate. Committee on Government Operations. Budgetary, organizational, and personnel data on departments and agencies performing police or investigative activities. Report (prepared by the Washington Regional Office of the General Accounting Office for Senator Charles H. Percy, Illinois). 94th Congress, 1st session, October 1975. (At head of title—Committtee print). Schedule I.

[73] Ibid.

Federal Units Performing Investigative or Police Activities

executive departments and agencies

Department of Agriculture—
- Office of Investigation.
- Forest Service.
- Security Force.

Department of Commerce—
- National Oceanic and Atmospheric Administration: National Marine Fisheries Service.
- Economic Development Administration.
- Maritime Administration: United States Merchant Marine Academy.
- National Bureau of Standards.
- Miscellaneous Offices—
  - Office of Minority Business Enterprise.
  - Office of Export Administration.
  - Office of Investigations and Security.

Department of Defense—
- United States Air Force.
- United States Army.
- United States Navy.
- United States Marine Corps.
- Defense Intelligence Agency.
- Defense Investigative Service.
- Defense Mapping Agency.
- Defense Supply Agency.

Department of Health, Education and Welfare—
- Division of Investigations.
- Social Security Administration, Investigations Branch, Office of Administration.
- Guard Force.
- Correctional Officers.

Department of Housing and Urban Development—Office of Inspector General.

Department of the Interior—
- Bureau of Mines.
- Bureau of Reclamation.
- United States Fish and Wildlife Service.
- Bureau of Land Management.
- Bureau of Indian Affairs.
- National Park Service.

Department of Justice—
- United States Marshals Service.
- Civil Disturbance Unit.
- Intelligence Unit—Organized Crime Section, Criminal Division.
- Immigration and Naturalization Service.
- Federal Bureau of Investigation.
- Bureau of Prisons.
- Drug Enforcement Administration.

Department of Labor—Office of Investigations.
Department of State—Security Office.
Department of Transportation—
Office of the Secretary.
Federal Aviation Administration.
United States Coast Guard.
Federal Railroad Administration.
Department of the Treasury—
Consolidated Federal Law Enforcement Training Center.
Bureau of Alcohol, Tobacco, and Firearms.
United States Customs Service.
Internal Revenue Service.
INTERPOL.[74]
Bureau of Engraving and Printing.
Bureau of the Mint.

OTHER UNITS

ACTION—Personnel Security Division.
Administrative Office of the United States Courts—Probation Service.
Agency for International Development—
Office of Inspections and Investigations.
Office of Security.
Office of Public Safety.

---

[74] INTERPOL, the acronym for International Criminal Police Organization, is an organization of 120 countries of which the United States is a member. That membership is maintained through the National Central Bureau/INTERPOL of the Department of the Treasury, which is staffed by personnel detailed from Treasury and the Drug Enforcement Agency, whose salaries are provided by the lending agency. INTERPOL is the communications system for law enforcement agencies among the member countries to transmit information and requests regarding specified criminal activities.

INTERPOL does not undertake any investigations itself and does not have an investigative force but member countries can request investigations through its offices to other nations.

The following description of INTERPOL procedures and the National Central Bureau (NCB)/INTERPOL relationship with the Federal Bureau of Investigation's National Crime Information Center (NCIC) was provided by David R. MacDonald, Assistant Secretary for Enforcement, Operations, and Tariff Affairs, Department of the Treasury, in testimony before a Senate Appropriations Subcommittee in 1975 (U.S. Congress. Senate. Committee on Appropriations. Subcommittee on Treasury, U.S. Postal Service, and General Government. International Criminal Police Organization (INTERPOL). Hearing 94th Congress, 1st session. May 6, 1975. pp. 6–7):

The FBI has granted the U.S. NCB access to the FBI's National Crime Information Center (NCIC). This access is granted pursuant to the guidelines established by the FBI for the protection of individual's rights and covers only those records containing information on: stolen securities; stolen motor vehicles; wanted persons (warrants outstanding); stolen, missing, or recovered guns; stolen boats; stolen license plates; and computerized criminal histories.

Director Clarence M. Kelley of the FBI has stated:

The NCIC is not, as some have alleged, a secret intelligence gathering network filled with loosely managed and frivolously gathered information concerning anyone coming to the attention of the police. It has indexed only the names of individuals for whom arrest warrants are outstanding or persons who have had substantial involvement, supported by fingerprint records, with the criminal police system.

Member countries of INTERPOL, U.S. law enforcement agencies or any other organization, person, et cetera, with whom the United States may come into contact within the course of carrying out its responsibilities, have no direct access to criminal records in the United States.

Requests from law enforcement agencies for information contained in the United States are evaluated individually by Federal agents assigned to the U.S. NCB and arrest or other information is provided as approved (1) by the agency from which the information is obtained and (2) by the responsible agent in the U.S. NCB. This is known as the "third agency rule," and applies to all exchanges of information between enforcement agencies.

The procedure within INTERPOL requires the requesting country to state the nature of its investigative request, which includes identifying its investigation and the reason for the request. If this is not stated along with the request, the receiving country will make a request for that information prior to transmitting the request. The request must be in accord with the laws of the country receiving the request, as well as being related to a criminal offense in both countries.

Energy Research and Development Administration[75]—Division of Safeguards and Security.
Environmental Protection Agency—Security and Inspection Division.
Farm Credit Administration—Examination Division.
Federal Reserve System—Physical Security Section
General Services Administration
Office of Investigations.
Federal Protective Service.
Government Printing Office—Security Service.
Library of Congress—Special Police.
National Aeronautics and Space Administration—Inspections and Security Division.
National Gallery of Art—Protection Staff.
Nuclear Regulatory Commission.
Canal Zone Government—
Customs Division.
Police Division.
Internal Security Office.
Panama Canal Company.
Small Business Administration—Security and Investigations Division.
Smithsonian Institution—Protection Services.
Tennessee Valley Authority—Patrol Force.
United States Capitol Police—Police Force.
United States Civil Service Commission—Bureau of Personnel Investigations.
United States Information Agency—
Physical Security Division.
Investigation Division.
United States Postal Service—
Office of Security.
Office of Criminal Investigations.
United States Supreme Court—Police Force.
Veterans Administration—
Investigation and Security Service.
Department of Medicine and Surgery.

The degree to which Federal investigative and police units employ surveillance technology is varied and depends upon the breadth of

---

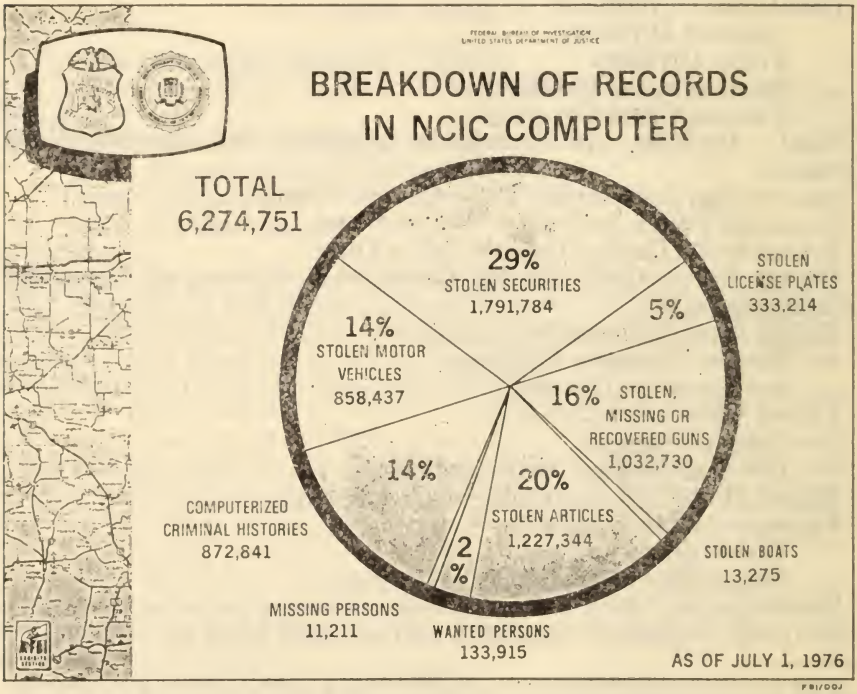
[75] The Atomic Energy Commission was abolished and its duties, functions, and authorities transferred to the Nuclear Regulatory Commission and the Energy Research and Development Administration by the Energy Reorganization Act of 1974 (88 Stat. 1233 and 1242). Both have certain responsibilities for the physical protection of nuclear materials, nuclear safety, and nuclear safeguards, some of which involve surveillance activities. ERDA's Division of International Security Affairs includes an Assistant Director for Intelligence Analysis, as noted above.

The International Atomic Energy Agency (IAEA), an international organization created in 1957 with a loose affiliation with the United Nations, has developed recommended guidelines for physical security and has established safeguards procedures for countries under IAEA safeguards. IAEA inspectors verify nuclear holdings in such countries and participate in certain relevant inspection practices.

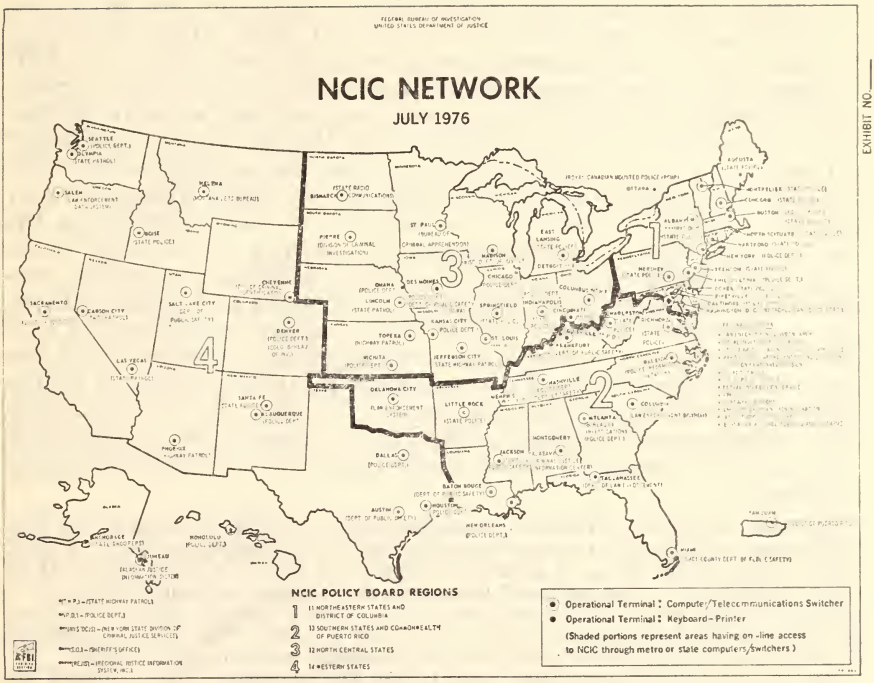
Sources include, inter alia, U.S. Congress. Senate. Committee on Government Operations. Nuclear weapons proliferation and the International Atomic Energy Agency. An analytical report prepared by Warren H. Donnelly and Barbara Rather of the Congressional Research Service. 94th Congress, 2d session. March 1976. William Doub and Joseph Dukert. Making nuclear energy safe and secure. Foreign affairs. Vol. 53. July 1975; Wojciech Morawiecki. IAEA's approaches to physical protection of nuclear materials. IAEA bulletin. Vol. 18, No. 1, 1976; and Systems of accounting for and control of nuclear material. IAEA bulletin. Vol. 17. April 1975.

their authority, responsibilities, and jurisdictions as well as their own internal dynamics and structures. However, given the availability and inherent utility of such technology for law enforcement, it is likely to be extensively used, whether in the form of television monitors and counter-intrusion devices to perform protective services or in the form of polygraphs and optical/imaging devices for investigative activities.

One critical and increasingly utilized information system is the computerized FBI National Crime Information Center (NCIC). NCIC systems comprise nearly 6.3 million records, containing information on wanted persons, stolen property, etc. It also includes the sensitive and controversial computerized criminal history (CCH) file. The potential abuse of this type of system reflects passive surveillance capability inherent in computerized criminal justice information systems. The following two figures illustrates the breakdown of records in the NCIC computer and the nationwide NCIC network.[76]



[76] Source: FBI.



A recent report by the General Accounting Office, entitled "FBI Domestic Intelligence Operations—Their purpose and Scope: Issues That Need To Be Resolved" (a copy of the digest is available in Chapter III, Section B.2),[77] provides an extensive review of appropriate FBI procedures, methods, techniques, and authorities. This GAO effort, the first examination of the FBI in its history, reviews the Bureau's use of surveillance technology in domestic intelligence operations. In addition to the NCIC, the FBI has maintained lists of individuals on several computerized indexes, with a heritage which dates to 1939—

1. Security Index—Individuals considered potentially dangerous to the United States. (Begun in 1943, terminated in 1971.)

2. Communist or Reserve Index—Individuals affiliated with the Communist Party, USA and/or revolutionary groups other than CPUSA. (1948–1971)

3. Administrative Index (ADEX)—Individuals considered a potential or actual threat to the United States, replaced the Security Index in 1971, when the Congress abolished the Emergency Detention Act and removed the statutory basis for the Security Index. (1971–1976)

4. Rabble-Rouser or Agitator Index—Individuals considered as contributors to civil disorders. (1967–1971)

5. Stop Index—Individuals of key interest to the Bureau in domestic intelligence, criminal, and espionage investigations and

[77] U.S. General Accounting Office. FBI domestic intelligence operations—their purpose and scope: issues that need to be resolved. Feb. 24, 1976. (GGD–76–50).

those wanted for FBI questioning. Stop Index was associated with the National Crime Information Center. (1971–1974) [78]

Other intelligence-gathering and investigative activities of the FBI include mail covers, openings, and interceptions; electronic surveillance, involving both wiretapping and bugging; and access to Federal income tax return information held by the Internal Revenue Service.[79]

Certain surveillance technologies require the cooperation of other entities, including those in the private sector. Some wiretapping by executive units, for instance, has relied upon the assistance of the American Telephone and Telegraph Company, a relationship which is currently under congressional investigation. That examination, conducted by the House Subcommittee on Oversight and Investigations, has resulted in an attempt by the Subcommittee to subpoena AT&T documents relating to warrantless wiretapping, a request which has been blocked by a Federal district court injunction, granted on the basis of Executive privilege asserted by President Ford.[80] Rep. John Moss, Chairman of the panel, stated the Subcommittee jurisdictional responsibilities and subsequent inquiry into warrantless wiretapping as follows:

> The subcommittee's jurisdiction over this matter is not "peripheral" as The Post contends (referring to a previous editorial in the Washington Post). Rule X of the Rules of the House of Representatives gives the most direct authority to this committee for "regulation of interstate and foreign communications". . . . Because of this responsibility, the subcomittee needs to learn what procedures are being used, if any, to safeguard the privacy of phone lines and to determine whether new law is needed restricting wiretapping without a court order.
>
> The value of the information sought by the Subcommittee is not "limited" as The Post contends. The records specify the places or phones to be tapped. They will indicate whether the subjects include news reporters and other private citizens, as some have alleged, or foreign embassies or aliens.[81]

The present inability of the subcommittee to secure this information clearly reflects the difficulty of assessing the magnitude and scope of surveillance technology utilization by the Federal government.

One of the principal surveillance methods is electronic eavesdropping, the interception of oral and wire communications. The Omnibus Crime Control and Safe Streets Act of 1968 (P.L. 90–351; 82 Stat. 211) provided for court authorization of electronic surveillance in order to effectively utilize this technology in crime control, and yet satisfy Fourth Amendment requirements. Title III of the 1968 statute requires annual reports regarding court-authorized eavesdropping and the subsequent reports provide a wealth of data about its utilization and utility, including information regarding costs, certain results, grants and denials. (A copy of the introduction to the "Report on the

---

[78] Ibid., pp. 66–77.

[79] Ibid. pp. 90–95. Elaboration of FBI surveillance activities is provided in at least two congressional hearings. U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Federal Bureau of Investigation. Hearings. 94th Congress, 1st sesssion. Nov. 18 . . . Dec. 11, 1975. ———. House. Select Committee on Intelligence. U.S. intelligence agencies and activities: domestic intelligence programs. Hearings. 94th Congress, 1st session. Oct. 9 . . . Dec. 10, 1975 (Part 3).

[80] Rep. John Moss, Chairman of the Subcommittee on Oversight and Investigations of the House Committee on Commerce. Security probes and security taps (Letter to the editor). Washington Post. Sept. 5, 1976. p. B6.

[81] Ibid. Another example of the incursion of executive privilege to withhold surveillance-related data and information is included in hearings investigating nonverbal communications interception. U.S. Congress. House. Committee on Government Operations. Subcommittee on Government Information and Individual Rights. Interception of nonverbal communications by Federal agencies. Hearings. 94th Congress, 1st and 2d sessions. Oct. 23, 1975 . . . March 11, 1976.

Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications for the Period Jan. 1, 1975 to Dec. 31, 1975" is included in Chapter IV. Section C, Courts.)

The 1975 report of the Director of the Administrative Office of the United States Courts [82] provided the following data regarding Federal court-ordered interceptions:

106 installations based on 108 authorizations;

1,589 total days in operation and an average of 18 days for each installation; [83]

$12,773 average cost per order (compared to $6,970 average cost per order for all Federal and State authorizations); [84]

an average of 71 persons intercepted, 1,100 intercepts, and 745 incriminating intercepts per order.[85]

A recent analysis on "Electronic Surveillance—Authorized Governmental Eavesdropping and the Numbers Game" [86] focused on the data elicited in the first seven years (1968–1974) of reporting the Omnibus Crime Control Act requirements. That examination discerned a number of findings regarding authorized electronic eavesdropping:

The data themselves are "inherently limited because they are statistical in nature and they exclude confidential material" [87] and those which do not require authorization, such as those surveillances for national security purposes. The data do not include those performed illicitly, or those consented to by one party;

in the six years of authorized federal eavesdropping only one application for an order was denied, which was in 1969, the first year of federal eavesdropping pursuant to Title III; [88]

the data indicate that applications for extensions of an order are usually granted. Only two federal and six state applications have been denied; [89]

approximately 64 percent and 43 percent of state interceptions were characterized as incriminating. From the almost 55,000 individuals overheard in federal installations, involving nearly 900,000 conversations, only 4,897 arrests and 1,985 convictions resulted. Thus, less than one of every 11 persons overheard was arrested, and less than one of every 27 was convicted of any offense; [90]

approximately one of every five suppression motions made subsequent to federal eavesdropping was granted. The data indicate that one of every 35 arrests resulted in suppression of at least part of the evidence obtained through the use of federal eavesdropping; [91] and

36 of 945 federal installations or four percent, were at least partially violative of Title III requirements.[92]

Warrantless electronic eavesdropping appears to be substantially greater than court-ordered surveillance. A report on "Electronic Surveillance" prepared for the 1973 Princeton conference on the FBI provided the following comments, quoting Senator Edward Kennedy in a letter addressed to members of the Senate Administrative Practices Subcommittee:

1. The number of federal wiretapping and bugging devices installed without court authorization is substantially greater than the executive branch has led the public to believe.

---

[82] Director of the Administrative Office of the United States Courts. Report of the Director on applications for orders authorizing or approving the interception of wire or oral communications for the period Jan. 1, 1975 to Dec. 31, 1975. (Washington) April 30, 1976.
[83] Ibid., p. VI (Table 2).
[84] Ibid., p. XII (Table 5).
[85] Ibid., p. X (Table 4).
[86] Electronic surveillance—authorized governmental eavesdropping and the numbers game (Note). Rutgers law review. Vol. 29, No. 2. Winter 1976.
[87] Ibid., p. 404.
[88] Ibid., p. 407.
[89] Ibid., pp. 408–409.
[90] Ibid., p. 413.
[91] Ibid., p. 417.
[92] Ibid., p. 418.

2. The average duration of such devices is many times longer than the average duration of court-approved devices.

3. As a result, the total amount of federal electronic eavesdropping without court permission far exceeds the eavesdropping with judicial approval.

4. There is strong reason to doubt the validity of the repeated public assurances by the Justice Department that it fully complies with the 1968 congressional standards before installing any tap or bug without a court order.

5. Despite the department's assertions to the contrary, there is an absence of well-defined procedures which would promote compliance with the statutory standards and permit meaningful congressional scrutiny of this extraordinary executive activity.[93]

The authors note that the Federal utilization of electronic eavesdropping is greater than public reports indicate because of Federal access to State and local electronic surveillance information, unreported national security wiretaps and buggings, unauthorized and illicit electronic surveillance, unreliable and possibly fraudulent reports on electronic surveillance, and possible use of electronic surveillance prior to court authorization.[94]

Further illustration of the magnitude of Federal utilization of surveillance technology includes various devices and equipment necessary for the conduct of relevant operations. An inventory of mechanical and/or electronic devices held by the Intelligence Division and the Inspection Service's Internal Security Division of the Internal Revenue Service [95] includes, among others, the following varied items: Miniature transmitters and recorders; miniature receivers; tape recorders; telephone induction coils; video cameras; miniature amplifiers; telephone analysers; base station radios; radio amplifiers and chargers; planetary and rotary microfilm cameras; surveillance trucks; illuminated filters for check unscrambling; and light amplification scopes.[96]

A final element of the scope and magnitude of direct Federal utilization and development of surveillance technology is the volume and extensiveness of Federal recordkeeping. According to the First Annual Report of the President, submitted in accordance to the Privacy Act of 1974, the following summary was filed:

> As of December 31, 1975, 85 (Federal) agencies subject to the Act had filed notices of 6,723 systems which they maintained containing more than 3.8 billion records about individuals.[97]

Nearly 87% of those records are held by twenty agencies; an additional 65 agencies hold fewer than 45 systems each.[98] The following chart identifies the agencies and records systems:

---

[93] Victor Navasky and Nathan Lewin, Electronic surveillance, In Pat Watters and Stephen Gillers (eds.). Investigating the FBI. New York, Doubleday. 1973. pp. 298–299.

[94] Ibid., pp. 299–302.

[95] U.S. Internal Revenue Service. Inventory of mechanical and/or electronic devices in custody of the Intelligence Division and the Inspection Service's Internal Security Division. U.S. Congress. House. Committee on Government Operations. Subcommittee on Commerce, Consumer, and Monetary Affairs. Oversight hearings into the operations of the IRS. Hearings. 94th Congress. 1st sesssion. May 14 . . . July 31, 1975. pp. 415–416. (Entire inventory included in Chapter IV, Section A. Executive Branch.)

[96] Ibid.

[97] Executive Office of the President. Office of Management and Budget. First annual report of the President (for calendar year 1975): Federal personal data systems subject to the Privacy Act of 1974. (Washington, D.C. 1976). p. 3. "A system of records is defined as a group of files of personal information about identifiable individuals from which information is retrieved by reference to name or some other personal identifier." Ibid.

[98] Ibid.

Summary of systems of records by agency [99]

Agencies:	*Systems*
Department of Agriculture	215
Department of Commerce	95
Department of Defense	2,141
Department of Health, Education, and Welfare	831
Department of Housing and Urban Development	57
Department of the Interior	278
Department of Justice	175
Department of Labor	73
Department of State	48
Department of Transportation	263
Department of Treasury	932
ACTION	62
Canal Zone Government	134
Central Intelligence Agency	57
Federal Communications Commission	68
General Services Administration	99
Postal Service	70
Securities and Exchange Commission	99
Small Business Administration	80
Veterans Administration	57
65 other agencies (those with fewer than 45 systems)	889
Total systems	6,723

Implicit in the manifold records systems and the immense quantity of individual records is a vast surveillance capacity. The collection of material for inclusion in the individual records systems reflects some utilization of surveillance technology. Moreover, the computerized records systems themselves represent a substantial potential for surveillance, especially in compiling personal dossiers.

By way of summary, direct utilization and development of surveillance technology by the Federal Government includes several distinct dimensions. Those elements are Federal Government . . .

Intelligence agency involvement, such as employment of relevant technologies and development of surveillance equipment and devices;

Law enforcement agency involvement, including monitoring for protective services and investigative surveillance;

Relationships with the private sector, as with the cooperative arrangements with AT&T;

Devices and equipment, including surveillance trucks and miniature transmitters; and

Adoption and development of specific technologies, including computerized recordkeeping systems, electronic eavesdropping, and wiretapping.

(2) *Technical assistance and grant support programs.*—Another aspect of the scope and magnitude of Federal involvement in surveillance technology is the technical assistance and grant support provided to subnational governmental units. Such efforts operate on the premise that most law enforcement is a State or local responsibility, rather than a national one, and, therefore, the Federal Government's role is relatively circumscribed. Consequently, Federal efforts in this area are restricted in terms of direct involvement but may be ex-

[99] Ibid.

panded in terms of assistance to other governmental units, especially with regard to funding of technology development and utilization programs and providing technical expertise and facilities.

Present supportive efforts to encourage the use of modern tools and techniques in the criminal justice community may be traced to some of the recommendations of the President's Commission on Law Enforcement and Administration of Justice established in 1965. The Commission's report, "The Challenge of Crime in a Free Society," provided the basis for the present direction of Federal funding to law enforcement and other criminal justice agencies.[100]

The recommendations of the Commission which relate to the issue of surveillance include the Federal sponsorship of science and technology research, development, and testing programs composed of three components—systems analysis, field experimentation, and equipment-system development.[101] Within the scope of the technology, as perceived in the mid-1960s, the report singled out the potential of two areas which have relevancy in surveillance—the semiautomatic fingerprint system and the development of automatic patrol car locators. The Commission also recommended that there should be a Federal agency assigned to coordinate the establishment of standards for equipment to be used by criminal agencies and to provide those agencies with technical assistance. Furthermore, the Commission suggested the development of a scientific and technological research program within a research institute framework that would "bring resources of science to bear on the problem of crime." [102]

Some of the concepts and specific recommendations of the Commission were brought to fruition by the enactment of the Omnibus Crime and Safe Streets Act of 1968 (Public Law 90–351). The Act created the Law Enforcement Assistance Administration (LEAA), which has been supportive of substantial infusions of technology to assist State and local law enforcement agencies. While there is some difficulty in pinpointing the exact LEAA expenditures for the purchase of surveillance technology and intelligence-related programs, an estimate by the Administration acknowledged an expenditure of grant funds of $160,810,447 over its first seven years of operation, representing 4.8% of the total amount of LEAA funding during that period.[103] The following statement from Richard Velde, Administrator of LEAA, details the funding:

> During the seven year period covered by the report, LEAA block and discretionary grant funds totalling $160,810,447 were used to support 1,929 projects related to intelligence. This represents 4.8% of the total dollar amount of LEAA funding during that time. 466 of these grants allocated $2,454,331 for the purchase of electronic surveillance equipment. This represents 1.5% of the total LEAA funds awarded for intelligence-related projects, and .07% of the total LEAA funding during the reporting period.
>
> Of the 466 grants allocating funds for electronic surveillance equipment, 299 grants involving $1,330,510 for surveillance equipment purchase, were made to

---

[100] U.S. President's Commission on Law Enforcement and Administration of Justice. The challenge of crime in a free society. Washington, U.S. Govt. Print. Off., 1967.

[101] Ibid., p. 270.

[102] Ibid.

[103] Richard Velde, Administrator, Law Enforcement Assistance Administration, in a letter to the Hon. Bella Abzug, Chairwoman, Subcommittee on Government Information and Individual Rights, House Committee on Government Operations, Jan. 22, 1976. Mr. Velde's statement introduced an LEAA report entitled "Survey of LEAA Funded Intelligence Related Grants—FY 1969 through 1975," Jan. 14, 1976.

states either prohibiting wiretapping or having no legislation on that subject at the time of award.[104]

An example of Federal assistance to subnational governmental units with regard to surveillance technology is the Computerized Criminal History (CCH) and other types of available records maintained in the FBI's National Crime Information Center (NCIC). In 1974 CCH information and records were reviewed by the General Accounting Office (GAO) for the Senate Subcommittee on Constitutional Rights.[105] The CCH system which became operational on Nov. 30, 1971, elicited the following GAO findings:

> When the Attorney General authorized the Federal Bureau of Investigation (FBI) to operate the CCH system in December 1970, he did not inform the FBI of (1) the extent to which certain criminal history information should have been maintained in Federal rather than State computers or (2) what type of advisory policy board should be established to review the policies and procedures used for CCH. He had, however, received recommendations regarding both matters from the Office of Management and Budget, Executive Office of the President.
>
> In the absence of such direction from the Attorney General, the FBI, with the concurrence of its National Crime Information Center Advisory Policy Board, developed the policy and operating procedures for CCH.
>
> There is some question as to the extent of computerized criminal history information which should be retained in the FBI's computers.
>
> Data is not available to indicate how computerized criminal history information has been used.
>
> Both the FBI and the Law Enforcement Assistance Administration have either funded, or seek to develop, telecommunication system capabilities, to allow State and local criminal justice agencies to exchange administrative messages more effectively. The development of two systems could result in duplication and an unnecessary expenditure of Federal funds. Moreover, the Attorney General has not decided whether the FBI has legal authority to operate such a system.[106]

The most recent General Accounting Office investigation of the FBI [107] found that in the interim (from 1974 to 1976) "the FBI ade-

---

[104] Ibid. The report itself elaborates upon the surveillance equipment awards. "Of the $1,211,502 awarded for electronic surveillance equipment, 44.2 percent or $535,139 for 59 grants was awarded to the following 20 states which, at the time of the award, prohibited wiretapping or had no legislation on the subject. . . . A preliminary review, of the legislative history of the above listed 20 states, indicates that electronic surveillance under proper consensual circumstances which is allowable under Paragraph 2511(2) of Title III, Public Law 90-351, would have been permissible in these states at the time of grant award." Law Enforcement Assistance Administration. Survey of LEAA funded intelligence related grants—FY 1969 through FY 1975. Jan. 14, 1976. (Washington, D.C.)
The equipment purchased by states utilizing organized crime discretionary grants included remote audio recorders, "beeper" vehicle trailing systems, surveillance transceivers and transmitters, audio bandpass filters, tone decoders, body transmitters, concealable transceivers and transmitters, and electronic surveillance kits. Ibid. Attachment 6 (unpaginated).

[105] U.S. General Accounting Office. Development of the computerized criminal history information system. Letter report and enclosure to Hon. Sam J. Ervin, Jr., Chairman, Subcommittee on Constitutional Rights, Senate Committee on the Judiciary. March 1974. (B-171019) (A copy of the letter report and enclosure are included in Chapter III, Section B.2. General Accounting Office reports.)

[106] Ibid., pp. 1-2 of letter report.

[107] U.S. General Accounting Office. FBI domestic intelligence operations—their purpose and scope, op. cit.

quately controlled dissemination of investigative information, but has not adequately examined its procedures for maintaining such data." [108] The GAO inquiry also specified that "in 18 percent of the cases in which information was disseminated (by the FBI to other agencies), it was given to State and local law enforcement agencies." [109] This assistance, which involves an element of surveillance technology, incorporates reciprocal benefits, since "State and local law enforcement agencies provided the FBI with information a great deal more often than the FBI provided the agencies with information." [110]

In measuring the magnitude and scope of Federal involvement in surveillance technology, both technical assistance and grant support to subnational governmental units are relevant ingredients. A somewhat related element is technology transfer.

(3) *Technology Transfer.*—Another aspect of the scope and magnitude of Federal involvement in surveillance technology is the development and transfer of appropriate technologies, devices, and equipment. Encouraged by both legislative requirements and administrative initiatives, criminal justice agencies have actively supported selective technological developments to assist in coping with criminal activity. In other instances, the technology developed by and for the military and national defense as well as the innovations from the space program [111] have been modified to meet criminal justice needs. Government use of surveillance technology has been further encouraged in part by the extensive funding efforts of the Law Enforcement Assistance Administration (LEAA) programs. Thus, various agencies have supported the diffusion of surveillance technology and related intelligence techniques through multiple and diverse technology transfer efforts.

One rationale for technology transfer is that public supported research and development should be ultimately useful to segments of society other than the Federal Government or particular agencies and should have utility in serving the "public good" in numerous ways. Space and military science developments epitomize this rationale. With regard to surveillance technology, both formal programs and informational exchanges have encouraged the dissemination of technological innovations. The active programs in technology transfer have involved the National Aeronautics and Space Administration, the Department of Defense, Law Enforcement Assistant Administration, Department of Commerce, and National Science Foundation.[112]

One illustration of technology transfer involves the Federal Laboratory Consortium, a group composed of representatives from government and industry, which has encouraged the diffusion of relevant

---

[108] Ibid., p. xiv.

[109] Ibid., p. 128.

[110] Ibid. The report found 70 cases of FBI distribution of information compared to 611 cases of FBI receipt of information from State and local law enforcement agencies.

[111] Examples of actual and potential technology transfer are included in publications of which excerpts are included in this collection. U.S. Congress, Senate, Committee on Armed Services, Special Electronic Battlefield Subcommittee of the Preparedness Investigating Subcommittee, Investigation into electronic battlefield program, Report, 92d Congress, 1st session, Feb. 22, 1971. U.S. Congress, Senate, Committee on Aeronautical and Space Sciences, Space benefits—the secondary application of aerospace technology in other sectors of the economy, 94th Congress, 1st session, April 16, 1975. (Both included in Chapter III, Section B.1, Excerpts from Congressional documents.)

[112] A detailed discussion of Federal support of technology transfer and diffusion efforts is found in a recent survey, Granville W. Hough, Technology diffusion: Federal programs and procedures, Mt. Airy, Maryland, Lomond Books, 1975, 406 pp.

technologies. At the Consortium's semi-annual meeting, held in June of 1976, some emphasis was placed on technological areas which had relevance for the law enforcement and criminal justice communities. The participants at the meeting identified some of the law enforcement related programs which were federally supported, a few of which have implications for police surveillance—cost-effective burglar alarm systems, speaker identification program, system of control of the illegal use of explosives, and cargo security systems.[113]

(4) *Training programs.*—Training programs by the Federal Government represent a final dimension of the scope and magnitude of Federal involvement in surveillance technology. The use of sophisticated surveillance devices and equipment requires highly trained operators. Relevant training is provided by the Federal Government for its own personnel and those of subnational governmental units.

Certain law enforcement, intelligence, and investigative agencies which utilize surveillance technology conduct some of their own training programs. Others are shared among agencies or contracted with private industry. One of the broader based training efforts at the national level is conducted by the Consolidated Federal Law Enforcement Training Center (CFLETC) of the Department of the Treasury. CFLETC was established by Treasury Department Order No. 217, effective March 2, 1970, and Revision 1, effective June 30, 1970. The Center serves 24 Federal law enforcement agencies representing 10 executive departments.[114] The extent of the Center's training services and clientele is summarized in the following description from the U.S. Government Manual:

> The Center conducts common recruit, advanced, specialized, and refresher law enforcement training for the special agents and police officers from the participating agencies, and provides the necessary facilities, equipment, and support for the accomplishment of that training. Also, the Center provides training on a space available basis to the law enforcement personnel of an additional 15 Federal agencies, to qualified civilian personnel from military agencies, and to the training personnel of various State and local law enforcement agencies. The recruit courses and other training for more than one agency are conducted by Center personnel, while specialized courses for recruits and the advanced, inservice, and refresher courses for the personnel of a single agency are conducted in the Center's facility by the personnel of the agency involved.
>
> The Center develops the curriculum content and training techniques for use in the recruit training, and advises and assists the participating agencies on the production and formulation of the materials and mechanics required for the various agencies' specialized training. Administrative support for the advanced and specialized training programs is provided by the Center's two schools—the Criminal Investigator School and the Police School.[115]

The Law Enforcement Assistance Administration (LEAA) in the Justice Department supports various training programs (for State and local law enforcement units). Those programs include the Law Enforcement Education Program (LEEP), the National Criminal Justice Education Consortium, the Graduate Research Fellowship Program, and the Internship Program. The internships, educational programs, and training programs provide a variety of services, some of which are related to surveillance technology utilization, and range

---

[113] Federal Laboratory Consortim. Notes on the semi-annual meeting. Naval Underwater Systems Center, Newport, Rhode Island. June 1976 (unpaginated).
[114] United States Government Manual, 1975/1976. U.S. Govt. Print. Off., 1975, p. 410.
[115] Ibid.

from legal-constitutional educational offerings to specialized instruction and participation in appropriate technologies.[116]

In sum, the scope and magnitude of Federal involvement in surveillance technology includes four basic dimensions—direct utilization and development of relevant technologies, technical assistance and grant support to subnational governmental units, technology transfer, and appropriate training programs. These resultant programs and operations cross a multiplicity of Federal agencies, include State and local government units and the private sector, and encompass a substantial diversity and proliferation of surveillance technologies, devices and equipment.

Federal support in surveillance and related technologies has not only included direct funding in the purchase of equipment but has undertaken to develop incentives for technology transfer, provided relevant training, contributed to the development of standards and equipment guidelines, and has stimulated and contributed to improving marketing of surveillance technologies by providing development funding.

While the total ramifications of government policies are beyond the scope of this report, it is significant to note that proliferation of surveillance techniques, which has been in part due to extensive funding in both the military and intelligence environments, has stimulated the growth of a large industrial complex. This is evidenced by the growing number of conferences on security and law enforcement technology, emergence of appropriate organizations, and the development of a distinct body of literature.

It is impossible to estimate costs of such Federal involvement principally because of the sensitivity of relevant operations and the resulting classified nature of the data. The following statement from the 1976 General Accounting Office report on the FBI identifies this handicap in measurement:

> In August 1975 Justice Department and FBI officials testified before the House Select Committee on Intelligence that the FBI spent about $82.5 million on general intelligence gathering in fiscal year 1975. However, the estimated amount includes money spent on FBI staff involved in criminal, domestic, and foreign intelligence operations, as well as payments made to informants in such operations. It does not include all funds spent on certain technical support associated with intelligence operations. Further breakdown of the amount is classified information.[117]

Since most Federal surveillance is conducted by intelligence and law enforcement agencies of the Federal government, a substantial part of the data associated with costs is excluded from public scrutiny because of imposed confidentiality and official secrecy. Moreover, an accurate estimate of the costs of surveillance technology would be impossible without inclusion of factors other than hardware per se—e.g., administrative support, research and development, personnel employment and training, maintenance and security of relevant equipment and devices, private sector assistance. Compounding the problem of securing valid and reliable estimates of total costs would be the difficulty of determining the costs of related enterprises (e.g., those in-

---

[116] Ibid., p. 322. See also U.S. Department of Justice. Attorney General's report on Federal law enforcement and criminal justice activities, 1975. Washington, D.C., 1975, pp. 184–190.

[117] U.S. General Accounting Office. FBI domestic intelligence operations—their purpose and scope, op. cit., pp. 131–132.

volved in technology transfer) and the costs attributable to related agencies, which might not be direct participants in the employment or generation of surveillance technology.

b. *Authorities and Standards.*—The authorities and standards associated with surveillance technology policy examined in this report are related primarily to the employment and utilization of the technology, not to the research and development of relevant technologies, equipment, and devices. Both authorities and standards vary among the agencies which manifest surveillance technology in part because of the independence of the agencies; their different responsibilities, duties, and functions; and the absence of comprehensive statutory controls over the use of surveillance technology.

Examples of the last factor—i.e., the lack of comprehensive legislative controls—should be noted initially. For instance, the Omnibus Crime Control and Safe Streets Act of 1968 (P.L. 90–351) established prohibitions on interception and disclosure of wire or oral communications by private parties or government officials without court authorization. However, certain Presidential powers to conduct electronic surveillance with respect to national security were exempted from the statutory requirements. Another illustration of exemptions is included in the Privacy Act of 1974 (P.L. 93–579). Although the 1974 Act provided for subject access to his or her records held by Federal agencies, certain law enforcement, investigative, and intelligence records have been excluded from the requirement.

(1) *Authorities.*—Authorities relating to surveillance technology policy include a series of alternatives, ranging from broad and somewhat nebulous statutory provisions to specific administrative directives. It has been recently emphasized that some of the authorizations have been based on uncertain or questionable authority. With regard to this last element, examinations have noted that certain uses of surveillance technology have been conducted without appropriate authorization or under debatable authority. For example, in 1975 Rep. Charles Wilson, Chairman of the House Subcommittee on Postal Facilities, Mail, and Labor Management, identified an absence of proper authority regarding mail openings by the CIA with the acquiescence of the Chief Postal Inspector, William Cotter, who was a former CIA employee:

> But the issue that is the most serious is the actual opening of the mail which was apparently conducted solely by the CIA.
>
> Mr. Cotter didn't reveal anything secret, but I expect a lot of people in the CIA were sensitive about having him talk about what they're doing, and I understand that.
>
> He acknowledged that they didn't know whether it was legal or not for the CIA to open mail, under the national security laws, but on his own decision, they went ahead with it and he was aware of what was being done.[118]

Another indication of surveillance technology utilization without proper authority involves the maintenance of material held by the U.S. Army Counterintelligence Analysis Detachment (CIAD) in the Counterintelligence Research Files System (CIRFC).[119] In fact, this

---

[118] U.S. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Postal Facilities, Mail, and Labor Management. Postal Inspection Service's monitoring and control of mail surveillance and mail cover programs. Hearings. 94th Congress, 1st session. May 6 . . . Nov. 5, 1975. p. 59.

[119] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Committee on Commerce. Special Subcommittee on Science, Technology, and Commerce. Surveillance technology. Hearings. 94th Congress, 1st session. June 23 . . . Sept. 10, 1975.

episode involves a breach of authority, as recounted in a report prepared by the Secretary of the Army, excerpts of which follow:

On January 10, 1975, I reported to the Congress that a microfilm library of an Army intelligence office in the Washington, D.C. area contained a substantial amount of information relating to the activities of American civilians not affiliated with the Department of Defense in apparent violation of the requirements of Defense Department Directive 5200.27 and Army Regulation 380–13. . . .

In 1971, the Army provided the Subcommittee on Constitutional Rights of the Senate Judiciary Committee its assurances that this particular file had been thoroughly screened and all nonretainable material destroyed. In addition, the June 1, 1971 Army letter imposed a requirement that all Army investigative files be reviewed annually in order to eliminate any documents pertaining to non-DoD-affiliated persons within the United States unless the information in these documents currently satisfied the criteria of DoD Directive 5200.27. Why, then, was this information still there?

The CIAD file was in fact screened in January, 1971, for the purpose of eliminating all material, retention of which was prohibited by the Army December 15, 1970, letter (copy enclosed), which was a precursor to DoD Directive 5200.27. The retention criteria of that letter were essentially identical to those of the Directive, and to those of the Army's June 1, 1971, letter, although the time period for judging the currency of the enumerated threats was not as specifically stated. That screening, however, apparently did not eliminate all information concerning unaffiliated civilians. While it is difficult now to reconstruct what happened, it appears that information regarding groups believed to have been seeking to develop opposition to the war in Vietnam among GI's or otherwise to pose a threat to the Army, was retained as authorized by the December 15 letter. In addition, the team apparently was instructed that information regarding the activities within the U.S. of suspected foreign intelligence agents and regarding foreign emigre groups within the U.S. would be retained, regardless of date, as meeting the "current relevance" requirement of the December 15 letter. In addition, the team apparently was instructed that information regarding the activities within the U.S. of suspected foreign intelligence agents and regarding foreign emigre groups within the U.S. would be retained, regardless of date, as meeting the "current relevance" requirement of the December 15 letter.

The subsequent commanders of CIAD apparently assumed that the January 1971, screening had eliminated all references to nonaffiliated civilians, not realizing that the material left in the file as retainable in January 1971, because the subject posed a then-current threat to the Army, was required to be rescreened annually to determine whether that threat continued to exist. This misunderstanding of the scope of the January 1971, purge and of the annual vertification requirements led to a failure to perform a thorough review of the microfilm holdings each year when the files were required to be verified for compliance with the Directive. This oversight was discovered in the late fall of 1974 by the present commander of CIAD in the course of his effort to apply the new file verification procedures established in AR 380–13.[120]

Further examples of uncertain or questionable authority for the use of certain surveillance technology are available throughout the Final Report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities.[121] FBI wiretapping and bugging provided evidence for such conclusions, as the Select Committee reported:

In 1940, President Roosevelt authorized FBI wiretapping against "persons suspected of subversive activities against the United States, including suspected spies," requiring the specific approval of the Attorney General for each tap and directing that they be limited "insofar as possible to aliens."

---

[120] Ibid., pp. 29 and 33.

[121] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Intelligence activities and the rights of Americans (Book II). Final report. 94th Congress, 2d session. April 26, 1976.

This order was issued in the face of the Federal Communications Act of 1934, which had prohibited wiretapping. However, the Attorney General interpreted the Act of 1934 so as to permit government wiretapping. Since the Act made it unlawful to "interpret *and* divulge" communications, Attorney General Jackson contended that it did not apply if there was no divulgence *outside* the Government. [Emphasis added.] Attorney General Jackson's questionable interpretation was accepted by succeeding Attorneys General (until 1968) but never by the courts.

Intrusive techniques such as bugging, mail opening and surreptitious entry were used by the FBI without even the kind of formal Presidential authorization and requirement of Attorney General approval that applied to warrantless wiretapping.

During the war, the FBI began "chamfering" or surreptitious mail opening, to supplement the overt censorship of international mail authorized by statute in wartime. The practice of surreptitious entry—or breaking-and-entering—was also used by the FBI in wartime intelligence operations. The Bureau continued or resumed the use of these techniques after the war without explicit outside authorization.

Furthermore, the installation of microphone surveillance ("bugs"), either with or without trespass, was exempt from the procedure for Attorney General approval of wiretaps. Justice Department records indicate that no Attorney General formally considered the question of microphone surveillance involving trespass, except on a hypothetical basis, until 1952.[122]

A final illustration of questionable (if not non-existent) authority regarding surveillance technology employment is the Federal Communications Commission monitoring of employees' telephones. A 1972 congressional investigation of alleged wiretapping by the FCC [123] revealed that secret surveillance was conducted with neither the requisite court order nor consent of the parties, despite statutory prohibitions to the contrary.[124]

Broad and/or nebulous authorities have also been associated with the use of surveillance technology, especially as conducted by law enforcement and intelligence agencies. Imprecise concepts, undefined terms, and ambiguous phraseology have complemented already far-reaching authorities granted to the President or relevant agencies either by statute or constitutional interpretation. (For a review of the interpretations by the Supreme Court, see the reports in Chapter III, Section B.3, "Wiretapping and Electronic Surveillance;" Chapter IV, Section A, "Electronic Surveillance and National Security Electronic Surveillance History, Policy and Procedure;" and Chapter IV, Section C. "State of the Law Relating to Wiretapping and Electronic Surveillance;" among others.)

Some of the findings of the President's Commission on CIA Activities Within the United States indicate the critical ambiguities associated with the CIA authority relating to domestic surveillance and use of relevant technologies.[125] The National Security Act of 1947 (Public Law 80–253), as amended, which created the Central Intelligence Agency, provided broad authorities—"the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure," and the CIA shall "perform such other functions and duties related to intelligence affecting the

---

[122] Ibid. pp. 36 and 38.

[123] U.S. Congress. House. Committee on Interstate and Foreign Commerce. Special Subcommittee on Investigations. FCC monitoring of employees' telephones. Hearings. 92d Congress, 2d session. March 28 and May 16, 1972.

[124] Ibid., pp. 9–10.

[125] U.S. President's Commission on CIA Activities Within the United States. Report. Washington, D.C. U.S. Govt. Print. Off., 1975. pp. 45–71.

national security as the National Security Council may from time to time direct"—while prohibiting other functions, namely, "internal security functions." As the Commission observed, however—

> The precise scope of many of these statutory and Constitutional provisions is not easily stated. The National Security Act in particular was drafted in broad terms in order to provide flexibility for the CIA to adapt to changing intelligence needs. Such critical phrases as "internal security functions" are left undefined. The meaning of the Director's responsibility to protect intelligence sources and methods from unauthorized disclosure has also been a subject of uncertainty. . . .
>
> Since the constitutional and statutory constraints applicable to the use of electronic eavesdropping (bugs and wiretaps) have been evolving over the years, the Commission deems it impractical to apply those changing standards on a case-by-case basis. The Commission does believe that while some of the instances of electronic eavesdropping were proper when conducted, many were not. To be lawful today, such activities would require at least the written approval of the Attorney General on the basis of a finding that the national security is involved and that the case has significant foreign connections.[126]

The Senate Select Committee on Intelligence examined the same authorities relating to CIA domestic electronic surveillance operations and concluded with the following observations and interpretations:

> These programs illustrated fundamental weaknesses and contradictions in the statutory definition of CIA authority in the 1947 Act. While the Director of Central Intelligence is charged with responsibility to protect intelligence "sources and methods," the CIA is forbidden from exercising law enforcement and police powers and "internal security functions." The CIA never went to Congress for a clarification of this ambiguity, nor did it seek interpretation from the chief legal officer of the United States—the Attorney General—except on the rarest of occasions.[127]

The breadth as well as the imprecision of authority to conduct electronic surveillance has been epitomized by the national security exemptions included in the Omnibus Crime Control Act of 1968 (P.L. 90–351). The relevant section (18 U.S.C. 2511 (3)) reads . . .

> (3) Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

The Senate select committee on intelligence concluded that "the imprecision and manipulation of labels such as 'national security,' 'domestic security,' 'subversive activities,' and 'foreign intelligence,' have led to unjustified use of these (intrusive) techniques."[128] An example may be found in the use of the "national security" justifi-

---

[126] Ibid., pp. 11 and 31.

[127] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Intelligence activities and the rights of Americans (Book II). Final report. 94th Congress, 2d session, April 26, 1976, p. 103.

[128] Ibid., pp. 183–184.

cation for the electronic surveillance of Executive officials and newspersons from 1969 to 1973.[129] According to the Senate committee—

> The "seventeen wiretaps" also show how the term "national security" as a justification for wiretapping can obscure improper use of this technique. Shortly after these wiretaps were revealed publicly, President Nixon stated they had been justified by the need to prevent leaks of classified information harmful to the national security.[130]

A final example of a broad authority relating to Federal utilization of surveillance technology provides another dimension—the cooperative relationship among agencies. In the aftermath of the assassination of Senator Robert F. Kennedy, while campaigning for the Democratic nomination for the Presidency, Congress passed Public Law 90–331, which provided, in part, for strengthened Secret Service protective authority:

> When requested by the Director of the United States Secret Service, Federal Departments and Agencies, unless such authority is revoked by the President, shall assist the Secret Service in the performance of its protective duties.

This statute provided the authority for Secret Service "watch list" requests for National Security Agency monitoring and electronic surveillance.[131]

In sum, authorities associated with various types of surveillance technology, especially electronic surveillance, have been found to be broad and ambiguous, resulting in extensive executive discretion and restrictions on legislative controls. Those authorities include exemptions to controlling legislation, imprecise and undefined terminology, possibly contradictory provisions, and wide-ranging related authorities.

(2) *Standards and guidelines.*—The standards and guidelines associated with surveillance technology, which are promulgated by Federal agencies, vary in terms of specificity, the technology and equipment included, and the scope of the units covered. The standards and guidelines may be broadly encompassing and general, such as the 1976 guidelines from the Justice Department dealing with various types of FBI investigations, or they may be relatively narrow and specific, such as the Internal Revenue Service's guidelines regarding inspection of Federal income tax returns by other Federal agencies. Elaboration and examples of the agency standards and guidelines are included in later chapters. (Chapter IV, Section A, "Executive Branch," includes material for a variety of agencies, including the Justice Department, Internal Revenue Service, and U.S. Postal Service, stating standards and guidelines for a number of surveillance technologies—electronic surveillance, personnel and domestic security investigations employment of surveillance technology, inspection of Federal income tax returns, information-gathering activities and

---

[129] Ibid., p. 122. "The relative ease with which high administration officials could select improper intelligence targets was demonstrated by the '17' wiretaps on Executive officials and newsmen installed between 1969–1971 under the rationale of determining the source of leakes of sensitive information. In three cases no national security claim was even advanced. While national security issues were at least arguably involved in the initiation of the other taps, the program continued in two instances against persons who left the government and took positions as advisors to Senator Edmund Muskie, then the leading Democratic Presidential prospect." Ibid.

[130] Ibid., p. 207.

[131] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. The National Security Agency and Fourth Amendment Rights. op. cit. pp. 11–12.

practices, and mail covers. Chapter IV, Section B, "Commissions," includes recommendations for improved or new standards and guidelines relating to particular surveillance technologies, such as Federal income tax return confidentiality, false identifications, wiretapping and electronic surveillance. Finally, Chapter V.C., "United Nations Documents," provides a 1974 report by the Secretary-General dealing in part with certain electronic surveillance systems, especially safeguarding electronic communications techniques.)

The 1974 report issued by the Secretary-General of the United Nations [132] examined a series of scientific and technological developments, including certain surveillance capabilities, and their impact on human rights. One of the major concerns was with the integrity of information stored on electronic data processing media (e.g., computerized criminal history records), and relevant safeguards. One of the recommendations in this area follows:

> A start might, however, be made in considering the possibility of drawing up international standards to ensure generally the integrity of information stored on electronic data processing media. These standards might provide, for example, for such measures as magnetic coding of tapes and other storage media with a view to protecting access to the information stored and safeguarding it from unauthorized alteration; and for setting up procedures for what is technically referred to as an "audit trail", which leaves a record of every access to and change made in the information stored.[132a]

A number of recent inquiries have examined and made recommendations regarding surveillance technology standards and guidelines. The President's Commission on CIA Activities within the United States recommended an Executive Order limiting CIA collection, evaluation, maintenance, and dissemination of information about the activities of American citizens;[133] Agency-issued guidelines for employees specifying permissible domestic activities, including surveillance practices: [134] and standards requiring that all files on individuals accumulated by the Office of Security in the program relating to dissidents should be identified and, with certain exceptions, destroyed.[135]

The National Commission on Wiretapping and Electronic Surveillance released its final recommendations in 1976, among which were several dealing with standards:

> Improved standards relating to recordkeeping by prosecutors regarding court-authorized electronic surveillance;
>
> Improved administrative standards surrounding consensual surveillance equipment use;
>
> Adoption of Federal court language which suggests standards regarding the "minimization" requirements associated with electronic surveillance under Title III of the Omnibus Crime Control Act of 1974 (P.L. 90–351);
>
> Development of new standards relating to the dissemination of electronic surveillance equipment and devices; and

---

[132] United Nations. Secretary-General. 1972–(Waldheim). Human rights and scientific and technological developments: uses of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society; report. New York, 1974. (United Nations. Document E/CN.4/1142/Add.2) (At head of title: United Nations Economic and Social Council)

[132a] Ibid., paragraph 85.

[133] U.S. President's Commission on CIA Activities Within the United States. op. cit. p. 13.

[134] Ibid., p. 19.

[135] Ibid., p. 27.

Statutory authorization for the Department of Justice to issue regulations defining specifically proscribed electronic surveillance devices manufactured and distributed by private manufacturers and to provide rules for maintaining inventory control.[136]

The 1976 General Accounting Office examination of FBI domestic intelligence operations recommended several improvements regarding surveillance technology standards, especially those related to the dissemination of FBI information.[137] The report noted the absence of written agreements between the FBI and State and local law enforcement agencies pertaining to the dissemination of information. Also identified in the report was the possible necessity of new standards relating to FBI dissemination of information to the Secret Service, because it may be unable to adequately evaluate the voluminous information.[138]

The Attorney General has recently issued guidelines relating to FBI domestic security investigations, White House personnel security and background investigation, and reporting on civil disorders.[139] Examples of some of the standards articulated in the memorandum dealing with domestic security investigations relate to surveillance technology application:

Investigative Techniques

Whenever the following investigative techniques are permitted by these guidelines, they shall be implemented as limited herein:

"Mail covers," pursuant to postal regulations, when approved by the Attorney General or his designee, initially or upon request for extension; and

Electronic surveillance in accordance with the requirement of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

Provided that whenever it becomes known that person(s) under surveillance are engaged in privileged conversation (e.g., with attorney), interception equipment shall be immediately shut off and the Justice Department advised as soon as practicable. Where such a conversation is recorded it shall not be transcribed, and a Department attorney shall determine if such conversation is privileged.

NOTE.—These techniques have been the subject of strong concern. The committee is not yet satisfied that all sensitive areas have been covered (e.g., inquiries made under "pretext;" "trash covers," photographic or other surveillance techniques.)

Dissemination

1. *Other Federal Authorities.*—The FBI may disseminate facts or information obtained during a domestic security investigation to other federal authorities when such information:

(a) Falls within their investigative jurisdiction;

(b) May assist in preventing the use of force or violence; or

(c) May be required by statute, interagency agreement approved by the Attorney General, or Presidential directive. All such agreements and directives shall be published in the Federal Register.

2. *State and Local Authorities.*—The FBI may disseminate facts or information relative to activities described in paragraph IB to state and local law enforcement authorities when such information:

(a) Falls within their investigative jurisdiction;

(b) May assist in preventing the use of force or violence; or

(c) May protect the integrity of a law enforcement agency.

---

[136] U.S. National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. Electronic surveillance. Report. Washington, D.C. U.S. Govt. Print. Off. 1976. pp. xv, xvi, xviii, xix.

[137] U.S. General Accounting Office. FBI domestic intelligence operations. . . . op. cit.

[138] Ibid., pp. 128–130.

[139] U.S. Department of Justice. Guidelines for domestic security investigations, White House personnel security and background investigations, and reporting on civil disorders and demonstrations involving a Federal interest. March 10, 1976 (Washington, D.C. [A copy of the guidelines is in Chapter IV. Section A, Executive Branch.]

3. When information relating to serious crimes not covered by paragraph IA is obtained during a domestic security investigation, the FBI shall promptly refer the information to the appropriate lawful authorities if it is within the jurisdiction of state and local agencies.

4. Nothing in these guidelines shall limit the authority of the FBI to inform any individual(s) whose safety or property is directly threatened by planned force or violence, so that they may take appropriate protective safeguards.

5. The FBI shall maintain records, as required by law, of all disseminations made outside the Department of Justice, of information obtained during domestic security investigations.[140]

A final element of Federal development of standards for surveillance technology utilization is that associated with State and local governmental criminal justice agencies. The Law Enforcement Standards Laboratory (LESL), a part of the National Bureau of Standards (NBS) Institute for Applied Technology, is a prominent entity involved in this activity. A description is provided in the LESL summary annual report for 1975:[141]

In "The Challenge of Crime in a Free Society," page 270, the President's Commission on Law Enforcement and Administration of Justice recommended that a Federal Government agency such as the National Bureau of Standards (NBS) be assigned the task of coordinating the development of standards for equipment used by criminal justice agencies, and the provision of technical assistance to these agencies.

This recommendation was implemented in January 1971 when, by means of a Memorandum of Understanding and an Interagency Agreement between NBS and the Law Enforcement Assistance Administration (LEAA), NBS established the Law Enforcement Standards Laboratory (LESL).

The mission of LESL is to assist law enforcement and criminal justice agencies in the selection and procurement of superior law enforcement equipment which is suited to their needs. It fulfills its mission by performing laboratory research on the performance of law enforcement equipment and serving as a national center of competence in this field of applied technology.

LESL activities include (1) the laboratory testing and evaluation of the performance of existing law enforcement equipment, (2) the development of methods for measuring the performance of this equipment, (3) the preparation of performance standards, user guidelines, and a variety of reports on the equipment and (4) service as a quick-response laboratory facility and panel of expert consultants.

The LESL operation has been funded at approximately two million dollars a year.[142]

LESL functions as a program manager and serves as an extension of the National Institute of Law Enforcement and Criminal Justice's (NILECJ) technical resources. (NILECJ is one of four offices in the Law Enforcement Assistance Administration and performs the research and development and technical assistance activities of LEAA and serves as a clearinghouse for the exchange of criminal justice information.) LESL has examined the state-of-the-art processes and has provided necessary standards in security systems as well as other law enforcement requirement areas, in an attempt to ensure that standards keep pace with the available improved equipment, especially that which has resulted as an outgrowth from aerospace and military technology.

---

[140] Ibid., pp. 4–6.

[141] Law Enforcement Standards Laboratory, National Bureau of Standards, Advanced Technology Division standards and guidelines program, Summary annual report, fiscal year 1975 (prepared for the National Institute of Law Enforcement and Criminal Justice, Law Enforcement Assistance Administration, U.S. Department of Justice) (Washington, D.C., 1976).

[142] Ibid., p. 1.

LESL is oriented to the development of performance standards, not design standards, and during its existence has produced twenty-four standards, three guidelines, thirty-three reports, and two reference materials.[143] Among the surveillance technology-related documents produced in fiscal year 1975, LESL developed a—

Standard for passive, first generation night vision devices (NILECJ–STD–0304.00);

Standard for active night vision devices (NILECJ–STD–0305.00);

LEAA police equipment survey of 1972, volume 4: alarms, security equipment, surveillance equipment (LESP–RPT–0004.00);

Report on electronic eavesdropping techniques and equipment (LESP–RPT–0207.00); and

Report on tests of hand-held metal weapon detectors for compliance with NILECJ–STD–0602.00.[144]

By way of summary, standards and guidelines, as with authorities relating to surveillance technology applications, have been neglected ingredients of policy until recently. Guidance concerning the employment of particular devices and equipment, control of specific technology development, utilization under prescribed conditions, and restrictions on the dissemination of the products of surveillance technology is determined to a substantial degree by the standards and guidelines promulgated by appropriate agencies. The specific standards translate broad legislative and executive authorities into practical implementation and, therefore, have an important policy determination. That determination increases in importance with regard to policy areas in which there is a substantial amount of administrative discretion due to the requisites of confidentiality and/or innovative and novel technological developments, as with surveillance technology.

The standards and guidelines promulgated by the Federal Government agencies demonstrate a diversity and variety reflective of the independence and responsibilities of the appropriate agencies. There appears to be, however, an increased awareness of a need to develop relatively specific guidelines and standards relating to the application of surveillance technology. The 1976 guidelines established by the Attorney General for certain FBI investigations followed revelations of FBI abuses regarding electronic surveillance, among other activities; and the efforts of Law Enforcement Standards Laboratory arose from a concern for effective utilization of improved and innovative surveillance technology.

To summarize this section on surveillance technology policy, it is important to review the major ingredients of the policy configuration. The authorities and standards developed for and by executive agencies interrelate with elements involved in defining the scope and magnitude of Federal policy—direct utilization and development, including law enforcement and intelligence agencies and operations; technical assistance and grant support, especially to subnational units; technology transfer programs among agencies; and training programs. These efforts, in combination, represent Federal sponsorship, support, and utilization of surveillance technology which spans a

[143] Ibid., p. 2.
[144] Ibid., pp. 5–6.

plethora and diversity of agencies, programs, and operations. The magnitude cannot be estimated in dollar amounts, in part because of the confidential nature of many of the operations. Nonetheless, the extensiveness and variety of Federal involvement can be acknowledged. The result appears to be a multiplicity of policies rather than a single, coherent policy. This section has provided a framework for description and preliminary analysis of this complex, evolving, and imposing policy area, one which is noted for its sophisticated and innovative developments and, until recently, limited public awareness of its scope, magnitude, and authorities.

2. Implications of Surveillance Technology

Because implications of surveillance technology are manifold, this section is designed to highlight some of the principal ones. Further elaboration is provided in the introductory section of this chapter and in the collections of materials included in several subsequent chapters. (Chapter IV, Section C, Courts; Chapter V, Section B, Civil Liberties Issues and Policy Implications; and Chapter V, Section C, United Nations Documents, supply numerous appropriate articles. The review and survey of congressional action relating to surveillance technology, contained in Chapter III, A., provides additional materials.)

Both William Colby,[145] former Director of Central Intelligence, and Clarence Kelley,[146] Director of the Federal Bureau of Investigation, in commenting upon their respective agency mandates, acknowledge the primacy of basic rights and freedoms for a democratic society. Clarence Kelley identifies the issue as follows:

> When considering the issue of the right of privacy, it is particularly important to be reminded that this is not a new idea. In fact, this right lies at the roots of our American heritage. Incensed reaction to the continuous infringement of the personal liberty of our early colonists gave birth to this Nation—and it has been the protection of our hardwon rights that has sustained our Republic through nearly two centuries.
>
> Freedom, of course, is what America is all about.[147]

William Colby emphasized several objectives in developing a "new concept of *responsible* American intelligence" [emphasis in original], saying:

> We will articulate better guidelines for intelligence, spelling out what it properly can do and what it will not do. We will insure that it is focused on foreign intelligence, and does not infringe the rights of our citizens.
>
> We will develop better supervision of intelligence by the Executive, by the Congress, and even, where necessary, by the judiciary. Better external supervision of intelligence will certainly generate intensive internal supervision, insuring that American intelligence complies with America's constitutional concepts.
>
> And we will develop better secrecy for those aspects of intelligence that really need it, while at the same time ending the old tradition of total secrecy of everything about intelligence. The stream, even flood, of intelligence secrets that have been exposed this past year has brought home to every American the fact that we must have better protection for those secrets we need to keep.[148]

---

[145] William Colby, Secrecy in an open society, The center magazine, v. IX, n. 2, Mar./Apr. 1976. [Text of this article appears in Chapter V, Section B.]

[146] Clarence Kelley, But so is the right to law and order, Trial, v. 11, Jan./Feb. 1975. [Text of this article appears in Chapter V, Section B.]

[147] Ibid., p. 23.

[148] William Colby, op. cit., p. 28.

The heightened concern about infringements on basic rights and liberties, to which Directors Kelley and Colby refer, is represented in two major Supreme Court decisions, principally *Katz* v. *United States*, 389 U.S. 347 (1967) and *Berger* v. *New York*, 388 U.S. 41 (1967). These decisions "declared the fourth amendment applicable to electronic surveillance . . . and (have) given leverage to the federal judiciary to control government eavesdropping." [149]

These developments recognize that there are a multiplicity of implications regarding the use of surveillance technology, most incorporating a constitutional question of some magnitude which remains to be settled definitively. The issues involving the constitutional rights and civil liberties of citizens residing in the United States are the most critical elements. However, they reflect only part of the questions to be resolved or reconciled. Other implications of surveillance technology and its utilization include:

Rights of U.S. citizens abroad;

Rights of U.S. Citizens in the Armed Forces and sensitive positions;

Rights of Federal employees in other non-military agencies and departments;

Rights of foreign nationals and non-resident aliens within the United States;

Potential conflict of basic constitutional rights inherent in this area;

Different purposes—e.g. law enforcement, intelligence, national defense and security—for which surveillance technology is operationalized;

Powers of the Chief Executive, acting as Commander-in-chief and/or declaring "national security" purposes;

The President's power to withhold surveillance-related information from Congress and the Judiciary under the concept of "executive privilege";

Covert versus overt surveillance technologies;

Innovations in the technology and their meaning for existing legislation, standards, and court decisions.

Because of the elaboration of some of these themes in the articles and documents included in this compendium and the lack of time to pursue the themes adequately in this discussion, the purpose of this section is limited to identifying and describing some of these implications, not in analyzing them. That identification, however, might serve as a framework for further examination of the complex phenomenon of surveillance technology and its implications.

a. *Constitutional Rights of U.S. citizens.*—As noted previously, the relevant basic constitutional rights of U.S. citizens are those articulated in the First, Fourth, and Fifth Amendments and implied in the concepts of the right of privacy and protection against a "chilling effect."

The Senate select committee on intelligence [150] criticized certain

[149] Developments in the law—the national security interest and civil liberties. Harvard law review, v. 85, n. 6, Apr. 1972. p. 1245. [Text of this article is included in Chapter V. Section B.]

[150] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Intelligence activities and the rights of Americans. Book II. Final report. op. cit.

"intrusive" surveillance techniques, such as bugging and wiretapping, for their indiscriminant and unlimited quality: "By their nature, wiretaps and bugs are incapable of a surgical precision that would permit intelligence agencies to overhear only the target's conversations."[151] Consequently, innocent parties may find their rights jeopardized, even under the most austere use of court-authorized electronic surveillance.

The violation of the rights of innocent victims is only part of a series of constitutional problems associated with different categories of individuals and groups exposed to surveillance technology. Other categories of citizens or groups include U.S. citizens traveling abroad; members of the Armed Forces or those involved in sensitive, confidential programs, operations, and activities; individuals accused of criminal conduct and/or under active investigation;[152] members of "dissident" organizations; and members or organizations operating "pursuant to the direction of a foreign power," as the language of the proposed Foreign Intelligence Surveillance Act of 1976 (S. 3197) reads. Associated with these different categories have been different controls and utilizations of surveillance technology.

One of the inherent difficulties in protecting an individual's constitutional rights in this area is simply discovering whether or not a right may have been violated. If the greatest concern is with surreptitious and covert surveillance, an individual who was overheard may remain ignorant of the potential infringement on his liberties. That possibility may exist unless or until he is indicted for a crime and/or the information gathered by the covert surveillance is admitted as evidence. Even the Privacy Act of 1974 (P.L. 93–579), which includes provisions for subject access to his records, contains specific exemptions for certain systems of records—e.g., investigatory material compiled for law enforcement purposes, maintained in connection with providing protective services to the President and others, and acquired for Federal employment purposes (sec. k)—and general exemptions of systems of records within an agency if they are maintained by the Central Intelligence Agency or "by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws" (sec. j).[152a]

The right of privacy is related to other constitutional guarantees, such as freedom of speech and of press, right of association and due process and against self-incrimination. However, it is a distinct and relatively recent constitutional construct. With regard to surveillance technology utilization, the right of privacy has become one of the principal constraints against possible constitutional encroachments. Justice Brandeis first raised the defense in his dissenting opinion in *Olmstead* v. *United States*, 277 U.S. 438, 473–474 (1928):

> Subtler and more far-reaching means of invading privacy have become available to the government . . . the progress of science in furnishing the Government

[151] Ibid., p. 198.

[152] The recent Justice Department guidelines for domestic security investigations distinguish among preliminary, limited, and full investigations, each of which has different criteria and guidelines, including employment of certain surveillance technologies. Preliminary or limited investigations cannot use mail covers or electronic surveillance. U.S. Department of Justice. Guidelines for domestic security investigations. (Washington, D.C.) Mar. 10, 1976.

[152a] In the 94th Congress, a number of proposals have been advanced to curtail these restrictions on subject access to his/her records held by Federal agencies. For a compilation, see Appendix A. Privacy bills introduced in the 94th Congress: index and digest.

with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Can it be that the Constitution affords no protection against such invasions of individual security?

The dual nature of the right of privacy—the "right to be let alone" and the "right to control information about oneself"—may be associated with different and distinct surveillance technologies. For instance, the "right to be let alone" pertains to direct and active surveillance capabilities, such as electronic eavesdropping, whereas the "right to control information about oneself" pertains to passive surveillance technologies, such as computerized record systems.

Some have suggested that a "chilling effect" may be the consequence of surveillance practices, especially the perceived employment of extensive and sophisticated technologies. The Senate select committee on intelligence concluded that such an effect has been the result of domestic intelligence operations and activities:

That these abuses have adversely affected the constitutional rights of particular Americans is beyond question. But we believe the harm extends far beyond the citizens directly affected. . . .

When Government infringes those rights instead of nurturing and protecting them, the injury spreads far beyond the particular citizens targeted to untold numbers of other Americans who may be intimidated.

Free government depends upon the ability of all its citizens to speak their minds without fear of official sanction. The ability of ordinary people to be heard by their leaders means that they must be free to join in groups in order more effectively to express their grievances. Constitutional safeguards are needed to protect the timid as well as the courageous, the weak as well as the strong. While many Americans have been willing to assert their beliefs in the face of possible governmental reprisals, no citizen should have to weigh his or her desire to express an opinion, or join a group, against the risk of having lawful speech or association used against him.[153]

As noted previously, these constitutional guarantees, whether explicit or implicit, vary for different groups of citizens. Individuals in the Armed Forces or in certain sensitive government occupations (or employees of private contractors involved in sensitive government programs) might encounter a different legitimate use of surveillance technology than would other citizens. One notable example, which epitomized the extent of that difference, revealed an investigation of the CIA Office of Security. The final report of the President's Commission on CIA Activities Within the United States related the incident:

An extreme example of how far an investigation can go occurred in the late 1960's. A CIA employee who attended meetings of a group which the Agency suspected of foreign left-wing support, had been privy to extremely sensitive classified information. Physical surveillance of the employee was conducted for almost one year. A surreptitious entry was made into the employee's apartment by cutting through the walls from an adjacent apartment so that microphones could be installed. Seven microphones were placed so that conversations could be overheard in every room of the apartment. A cover was placed on the employee's mail for two months during one period and five months during another. Several of the subject's tax returns were also reviewed. This investigation yielded no evidence of disloyalty.[154]

The President's Commission concluded that similar investigations and electronic surveillance were a legitimate and lawful exercise of

[153] U.S. Congress. Senate. Select Committee to Study Governmental Operations . . . Final Report. Book II. op. cit., pp. 290–291.

[154] U.S. President's Commission on CIA Activities Within the United States, op. cit., p. 163.

the personnel investigative authority of the Director to protect intelligence sources and methods from unauthorized disclosure, "unless their principal purpose becomes law-enforcement or the maintenance of internal security." [155] Those same investigative powers and subsequent employment of surveillance technologies would vary for newspersons and other citizens not affiliated with the Agency, according to the Commission's conclusions.[156]

b. Rights of Non-Resident Aliens and Foreign Nationals.—Nonresident aliens and foreign nationals in the United States differ from U.S. citizens in the constitutional protections surrounding surveillance in the United States. Certain First Amendment rights are restricted for aliens and, according to one commentator, "aliens charged with espionage have fared no better with Fourth Amendment claims." [157]

The complicated constitutional questions surrounding the status of nonresident aliens and foreign nationals has been observable in commentary on the proposed Foreign Intelligence Surveillance Act of 1976 (S. 3197). The bills provision for warrantless electronic surveillance is applicable to "agents of a foreign power," defined in one category as an "officer or employee of a foreign power but not a permanent resident alien or citizen of the United States." Attorney General Levi in supporting the proposed legislation affirmed:

> That it will be the policy and intent of the Department of Justice, if this bill is enacted, to proceed exclusively pursuant to judicial warrant with respect to all electronic surveillance against domestic communications of American citizens or permanent *resident aliens.* (Emphasis added.)[158]

The implication is two-fold—(1) non-resident aliens have different rights than U.S. citizens with regard to surveillance and particular surveillance technologies and (2) administrative, statutory, and judicial controls over certain surveillance technologies are implemented differently with regard to non-resident aliens vis-a-vis U.S. citizens.

c. Potential Conflict of Basic Rights.—Another potential problem with surveillance technology, as defined in this paper, is associated with public disclosure of personal records maintained by the Federal Government. Modern information technology, improved surveillance technologies, and potential accessibility to the resultant massive files of personal records held by Federal agencies constitute a threat to the privacy of the individual in terms of disclosure of such information. The consequence of this concern was passage of the Privacy Act of 1974 (P.L. 93–579) which provides for subject consent before the disclosure of his/her records to those who do not have a "right to know."

On the other hand, particular societal rights inherent in a democracy, such as freedom of the press and public disclosure of Government-held information, suggest a potential conflict in certain instances.

One manifestation of that conflict was indicated in a recent review, prepared by the Congressional Research Service, of the administration

---

[155] Ibid., p. 165.
[156] Ibid., pp. 164–165.
[157] Christopher Pyle. A bill to bug aliens. The nation, May 29, 1976. Reprinted in U.S. Congress, Senate, Committee on the Judiciary. Foreign Intelligence Surveillance Act of 1976. Report together with additional and minority views (to accompany S. 3197). 94th Congress, 2d session. p. 159.
[158] U.S. Congress, Senate, Committee on the Judiciary, Subcommittee on Criminal Laws and Procedures. Foreign Intelligence Surveillance Act of 1976. Hearings. 94th Congress, 2d session. Mar. 29, 30, 1976. 13.

of the Freedom of Information Act (5 U.S.C. 552).[159] The analysis discovered that some executive branch entities relied upon the Privacy Act to restrict access to records they maintained:

> While the Privacy Act was not intended to restrict access to records available under the Freedom of Information Act (5 U.S.C. 552a(b)(2)), five Executive Branch entities—the Department of Housing and Urban Development, Department of Labor, Commission on Civil Rights, General Services Administration, and National Aeronautics and Space Administration—cited the Privacy Act when invoking the FOI Act exemption pertaining to statutory prohibitions on disclosing certain Government information (5 U.S.C. 552(b)(3)). One of these units, the Department of Labor, acknowledged that it is now aware of this practice being an improper action.[160]

d. *Purposes of Surveillance Technology Utilization.*—The Omnibus Crime Control Act of 1968 (P.L. 90–351) recognized that different purposes of surveillance elicit different controls over the utilization of particular technologies. The most important exemption to the Act's requirement for court-authorized warrants is that of "national security," which remains an elusive concept.

One possible implication of this exemption is that certain surveillance technologies will be more extensively used for some purposes than for others. Electronic surveillance, which requires a court order in domestic investigations and intelligence-gathering, except for "national security purposes," might exist in a larger percentage of the "national security" cases than in other types of cases. This implication has been corroborated by one of the conclusions of the Senate select committee on intelligence:

> In the absence of effective outside control, highly intrusive techniques have been used to gather vast amounts of information about the entirely lawful activities—and privately held beliefs—of large numbers of American citizens. The very intrusiveness of these techniques demands the utmost circumspection in their use. But with vague or non-existent standards to guide them, and with labels such as "national security" and "foreign intelligence" to shield them, executive branch officials have been all too willing to unleash these techniques against American citizens with little or no legitimate justification.[161]

The concern for balancing the purposes of national security and foreign intelligence production with the protection of civil liberties is reflected in the debates surrounding the Foreign Intelligence Surveillance Act of 1976 (S. 3197). According to its supporters, it recognizes that tension and complexity:

> Striking this balance between the need for such surveillance and the protection of civil liberties lies at the heart of S. 3197. As Senator Kennedy stated in introducing the legislation:
>
> "The complexity of the problem must not be underestimated. Electronic surveillance can be a useful tool for the government's gathering of certain kinds of information; yet, if abused, it can also constitute a particularly indiscriminate and penetrating invasion of privacy of our citizens. Our objective has been

---

[159] U.S. Library of Congress. Congressional Research Service. The administration of the Freedom of Information Act: a brief overview of executive branch annual reports for 1975. Multilith prepared by Harold C. Relyea, Sept. 2, 1976 (no. 76–166G) [Washington, D.C.].

[160] Ibid., p. 25. Another indication of a conflict of societal and individual rights in this area is acknowledged between the First Amendment, freedom of the press provision and individual privacy rights. See Comment. An accommodation of the privacy interests and First Amendment rights in public disclosure cases. University of Pennsylvania law review, v. 124. Jan. 1976.

[161] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Final report. Book II. op. cit., p. 209.

to reach some kind of balance that will protect the security of the United States without infringing on our citizens' human liberties and rights."[162]

Opponents of S. 3197 disagree, citing the imprecision and ambiguity of "foreign intelligence" and "national security" purposes.[163]

e. *President's "Inherent Power" to Utilize Surveillance.*—The constitutional question of the President's "inherent power" to conduct warrantless surveillance is another evolving concept, lacking definitive judicial interpretation.

In a recent correspondence with Senator Edward Kennedy, Attorney General Levi asserted that "the Executive may conduct electronic surveillance in the interest of national security and foreign intelligence, and in aid of his conduct of the nation's foreign affairs, without obtaining a judicial warrant."[164] Title III of the Omnibus Crime Control Act of 1968 (Public Law 90–351) contains provision for "the constitutional power of the President to take such measures as he deems necessary to protect the Nation . . . to obtain foreign intelligence information deemed essential to the security of the United States."

A 1976 review, conducted by the Senate Judiciary Committee, of the precedents and decisions of the Federal courts dealing with an inherent power of the President to engage in or authorize unwarranted surveillance concluded that:

> The validity of such surveillances and the existence of the constitutional limits on the President's powers to order such surveillances remain an open question. Without legislation on the subject, there is a possibility that future administrations will again assert the right to engage in warrantless surveillance, where foreign relations or national security is involved, against targets who may or may not have any link with a foreign power.[165]

Also noting the continuing constitutional quandary, the Senate select committee on intelligence concluded that there is no inherent Presidential power in this area:

> However, while the constitutional issue has not been resolved, the Committee does not believe that the President has inherent power to authorize the targeting of an American for electronic surveillance without a warrant. Certainly, if Congress requires a warrant for the targeting of an American for traditional electronic surveillance or for the most sophisticated NSA techniques, at home or abroad, then the dangerous doctrine of inherent Executive power to target an American for electronic surveillance can be put to rest at last. The Committee also would require that no American be targeted for electronic surveillance except upon a judicial finding of probable criminal activity. Targeting an American for electronic surveillance in the absence of probable cause to believe he might commit a crime is unwise and unnecessary.[166]

f. *"Executive Privilege."*—The President's power to withhold surveillance-related information under the concept of "executive privilege" has been and will likely continue to be an important element in this area.

Executive privilege refers to the order of the President preventing disclosure of material or information, the release of which he may judge to be detrimental to the national security. Various types of

---

[162] U.S. Congress. Senate. Committee on the Judiciary. Foreign Intelligence Surveillance Act of 1976. Report. op. cit., p. 11.
[163] Ibid., pp. 131 and 135.
[164] Ibid., p. 12.
[165] Ibid., p. 18.
[166] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Final report. Book II. op. cit., p. 325.

executive privilege have been noted by the Supreme Court in determining the constitutionality of the President's claim in response to legitimate congressional needs for information and documentation. Since judicial intervention into this area is most recent, beginning in the Watergate era, it is unclear how far Executive privilege and competing congressional claims utilizing the subpoena power extend. In *United States* v. *Nixon*, 418 U.S. 683, the Supreme Court intimated that military, diplomatic, or sensitive national security material might not be subject to congressional demands and might be protected by the claim of Executive privilege.[167] Such a decision might depend upon the determination of how compelling are the congressional needs for such information. Judicial resolution of the conflict is likely to remain on a case by case basis.

Since surveillance technology and its utilization are often involved in national security, military affairs, and foreign intelligence areas, the incursion of "executive privilege" is likely. Recently, in fact, a Federal district court judge enjoined a subpoena from the House Oversight and Investigations Subcommittee seeking information about American Telephone and Telegraph Company's role in warrantless wiretapping. The basis of the injunction was President Ford's claim of Executive privilege regarding AT&T's involvement in warrantless wiretapping pursuant to Presidential request.[168]

g. *Covert Versus Overt Surveillance Technologies.*—The Senate select committee on intelligence distinguished between covert and overt investigative techniques based upon the subject's awareness of the investigation.[169] An analogous distinction can be developed between

---

[167] *United States* v. *Nixon*, 418 U.S. 683 (1974), while rejecting an unqualified presidential privilege of immunity from judicial process in a criminal proceeding, sustains the existence of the Executive privilege "to the extent [it] relates to the effective discharge of a President's powers . . ." 418 U.S. at 711.

"In this case the President challenges a subpoena served on him as a third party requiring the production of materials for use in a criminal prosecution; he dies so on the claim that he has a privilege against disclosure of confidential communications. He does not place his claim of privilege on the ground they are military or diplomatic secrets. *As to those areas of Art. II duties* the courts have traditionally shown the utmost deference to Presidential responsibilities. In *C&S Air Lines* v. *Waterman S. S. Corp.*, 333 U.S. 103, 111 (1948), dealing with Presidential authority involving foreign policy considerations, the Court said:

" 'The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs has available intelligence services whose reports are not and ought not to be published to the world. It would be intolerable that courts, without the relevant information should review and perhaps nullify actions of the Executive taken on information properly held secret.'

"In *United States* v. *Reynolds*, 345 U.S. 1 (1953), dealing with a claimant's demand for evidence in a damage case against the Government the Court said:

" 'It may be possible to satisfy the courts from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged. When this is the case the occasion for the privilege appropriate and the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone in chambers.' Id., at 10.

"No case of the Court, however, has extended this high degree of deference to a President's generalized interest in confidentiality. Nowhere in the Constitution, as we have noted earlier, is there any explicit reference to a privilege of confidentiality, yet to the extent this interest relates to the effective discharge of a President's powers, it is constitutionally based." Id., at 710–711.

For a review of the complexities and constitutionality of executive privilege, see Raoul Berger. Executive Privilege: A Constitutional Myth, Cambridge, Mass. Harvard University Press. 1974; Adam Carlyle Breckinridge. The Executive Privilege: Presidential Control Over Information, Lincoln, Nebraska. University of Nebraska Press, 1974; and Mary Louise Ramsey, "Executive Privilege: Withholding Information from the Congress—Selected Issues and Judicial Decisions," Congressional Research Service Multilith 75–127A (April 3, 1975). Recent court decisions are *Senate Select Committee on Presidential Campaign Activities* v. *Nixon* (C.A.D.C.), 498 F. 2d 725 (1974), in addition to *United States* v. *Nixon*, 418 U.S. 683 (1974).

[168] See notes 80 and 81, supra.

[169] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Final report. Book II. op. cit., p. 324.

covert and overt surveillance technologies, the former including electronic surveillance and mail covers and openings and the latter including polygraphs.

The Senate select committee concluded that covert investigative techniques (surveillance technologies) were more intrusive than overt techniques. "The objective of these recommendations (dealing with domestic security investigative techniques) . . . is to ensure that the more intrusive the technique, the more stringent the procedural checks that will be applied to it." [170]

However, although overt surveillance technology may not be as intrusive as covert, overt technology may possess other similar characteristics—an indiscriminant and unlimitable quality. For instance, television monitoring of individuals frequenting certain Federal buildings is not selectively utilized in all cases or circumstances. Nonetheless, even this usage in the public domain is less likely to invade the rights of privacy of individuals than usage which "affords access to and permanent recordation of private property and activity" as with police helicopter surveillance and other aided observations.[171] According to a law review comment by John Kornoff:

> Application of the physical presence test of 'plain view' to police helicopter and other aided observations can lead to invasions of our reasonable expectations of privacy, in violation of the fourth amendment.
>
> Aerial surveillance, particularly when coupled with other visual aid devices, makes it unreasonably burdensome on citizens to insure that their private indiscretions . . . will not be subjected to government security.[172]

The importance of distinguishing between visual and audio surveillance and implicitly between covert and overt surveillance technologies is affirmed by the author in his conclusion:

> Unless some distinction can be drawn between audio and visual preceptions, the use of visual devices should likewise be proscribed where they intrude into a reasonable expectation of visual privacy. Courts have not applied the wisdom of the auditory surveillance concepts to visual observations aided by extra-sensory devices. One possible explanation for the judicial reluctance is that, until very recently, extra-sensory visual surveillance devices were not capable of the insidious intrusions made possible by micro-miniaturized microphones and other wiretapping equipment used for auditory surveillance.[173]

h. *Innovations in Surveillance Technology.*—As noted above, Justice Brandeis, in his dissent in *Olmstead* v. *United States*, 277 U.S. 438 (1928), anticipated novel and inventive surveillance technologies beyond wiretapping, which would jeopardize individual rights. The prophetic nature of his apprehension was confirmed in the recent report by the Senate select committee on intelligence:

> Given the highly intrusive nature of these techniques (e.g., electronic surveillance, mail openings), the legal standards and procedures regulating their use have been insufficient. Scientific and technological advances have rendered traditional controls on electronic surveillance obsolete and have made it more difficult to limit intrusions. Because of the nature of wiretaps, microphones and

---

[170] Ibid.

[171] John Jay Kornoff. Police helicopter surveillance and other aided observations: the shrinking reasonable expectation of privacy. California western law review, v. 11. Spring 1975. p. 505.

[172] Ibid., p. 506–507.

[173] Ibid., p. 527–528.

other sophisticated electronic techniques, it has not always been possible to restrict the monitoring of communications to the persons being investigated.[174]

Current developments in surveillance equipment and devices, such as microwave transmission, thermal image cameras, and acoustic sensors, have been delineated above. These impressive equipment developments have accompanied or have included other qualitative transformations—miniaturization, improved quality, enhanced processing, reduced costs per item, modularity, and remote control. The implication of the surveillance technology innovations has been to improve the surveillance function, while, at the same time, reduce the risk of discovery.[175]

The implications of surveillance technology innovations and their consequences are manifold. A number relate to the international sphere and intelligence production abroad, for which one observer has recognized that "in light of revolutionary improvements in the technology of intelligence collection, more old methods (e.g. agent operations) should be retired." [176]

Some of the implications of technological innovations for control of domestic uses of surveillance technology and protection of constitutional rights have been raised in recent congressional discussions on the proposed Foreign Intelligence Surveillance Act of 1976 (S. 3197). The bill's definition of "electronic surveillance" includes "mechanical" and "other surveillance devices" but does not elaborate or catalogue relevant items. Critics of S. 3197 have suggested that directions and criteria for judicial authorization of these other surveillance devices (e.g. television monitors) require delineation because the newer technology may have made obsolete standards and criteria for "interception of wire and oral communications," included in the controlling Title III of the Omnibus Crime Control Act of 1974.[177]

The increased intrusiveness, yet reduced risk, of contemporary surveillance technology suggests serious impediments to discovery by affected parties, especially innocent victims. The possibility of incidental overhears and surveillance of innocent parties expands under such conditions. Even the testing and experimentation with innovative devices constitutes a greater threat than in previous periods, as a result of its intrusiveness and limited detectability. Infra-red cameras and other night vision devices, for instance, which might be valuable police equipment, exemplify the apprehension about technological abuse or utilization in unauthorized areas—e.g., industrial espionage and invasion of personal privacy in the home.

In summary, the implications regarding surveillance technology cross a spectrum of areas, including, but not limited to, constitutional rights of U.S. citizens; protection afforded to foreign nationals in the United States; legislative, judicial, and administrative controls; Presidential power; and innovations in the technology per se.

---

[174] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Final report. Book II. p. 183.

[175] For a concise statement of the reduced risks, see Herbert Scoville, Jr. The technology of surveillance. Society, v. 12, Mar./Apr. 1975.

[176] Ibid., p. 63. See also Herbert Scoville, Jr. Is espionage a necessary instrument for intelligence gathering? Center report, v. IX, Apr. 1976.

[177] See remarks of Senator John Tunney in minority views of report on S. 3197 in U.S. Congress. Senate. Committee on the Judiciary. Foreign Intelligence Surveillance Act of 1976, op. cit., pp. 133–135.

E. Controls and Oversight

1. Ingredients and Purposes

The dangers inherent in the use of surveillance technology coupled with revelations of abuses involving such technology have stimulated an awareness of the need to apply appropriate and stringent controls and oversight. In a democratic society, the dilemma between the need for legitimate law enforcement and intelligence activities and protection of individual rights and liberties has been manifested in the discussions surrounding controls over surveillance technology. James Madison, writing in Federalist #51, recognized the basic dilemma at the time of the ratification of the Constitution:

> In framing a Government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place, oblige it to control itself.[178]

In that important paper, Madison defends the principles of checks and balances and separation of powers, suggesting that control and oversight is a shared responsibility. Legislative mandates, authorities, and standards; administrative regulations, guidelines, and rules; and judicial decisions and opinions impose direct controls over the use of surveillance technology. Furthermore, citizen participation and public inquiry may produce a significant impact.

This section highlights some of the controls and oversight applied to surveillance technology. Further elaboration is available in the previous section dealing with policy and implications as well as in later chapters. (Chapter III contains a substantial amount of material relating to legislative oversight, including a review of recent congressional actions, excerpts from congressional documents, and reports from the General Accounting Office and the Congressional Research Service. Chapter IV. B provides selections from various commissions, many of which advise improved or increased governmental controls and oversight regarding surveillance technology.)

The concept of oversight ranges across a spectrum of activities—from review and monitoring of administrative actions to supervising and controlling such behavior. Oversight enables responsible Government officials to understand the operations and activities of agencies and units under their authority while providing a system of accountability and a rational foundation for future action and decisions. Legislative oversight of administration [179] ideally permits the elected representatives of the public to ensure the accountability of non-elected administrators and to guarantee compliance with constitutional dictates. Furthermore, oversight may provide the capacity to ensure administrative compliance with legislative intent, to assure proper accounting of expenditures, to discover malfeasance in office

---

[178] Alexander Hamilton, James Madison, and John Jay. The Federalist Papers. New York, the new American library edition, 1961. p. 322.

[179] Among numerous other sources, the following recent publications provide a comprehensive review of legislative oversight. Morris Ogul. Congress oversees the bureaucracy: studies in legislative supervision. University of Pittsburgh Press. Pittsburgh, 1976. U.S. Congress. Senate. Committee on Government Operations. Subcommittee on Oversight Procedures. Congressional oversight: methods and techniques. (Prepared by the Congressional Research Service and the General Accounting Office). July 1976; and Legislative oversight and program evaluation: a siminar sponsored by the Congressional Research Service. U.S. Govt. Print. Off. Washington, D.C. May 1976.

and curtail arbitrary and abusive exercise of bureaucratic authority, and to check wasteful, excessive expenditures.

Reflecting the separated and fragmented policy-making environment and multiple policies surrounding surveillance technology, oversight is similarly dispersed among numerous entities. Variations in the degree of control and review are evident in this system.

One of the reasons for the disparity and differentiation is the impossibility of imposing comprehensive controls over surveillance technology, given the varied responsibilities and functions of the numerous relevant agencies and variety and innovative quality of surveillance devices, equipment, and technologies. As an example, recent legislative measures have tended to focus on specific surveillance technologies or its employment in particular contexts or for particular purposes—e.g., wiretapping, criminal justice information, personal data, foreign intelligence surveillance, surveillance by the Armed Forces. Existing legislation in the field often provides important exemptions, such as for "national security" or "foreign intelligence" purposes; and Presidents have utilized the concept of "executive privilege" to preclude public, judicial, and congressional scrutiny of certain activities associated with surveillance technology. Moreover, Federal courts have failed to adopt definitive decisions regarding surveillance technology employment, relying instead on specialized rulings determined by the particular type of surveillance technology employed, the characteristics of the affected parties, and purpose for which the technology is adopted.[180]

2. Legislation and Proposals

Increased openness in Government and other institutions appears to have evolved as an essential requirement of a modern democratic society. As the scope of governmental activity increases and its authorities and consequent requirements expand, the activities and actions of Government become more important and far-reaching. Thus, both the public and the individual citizen has needed increasingly more information to understand fully the impact of governmental policies and practices on everyday life. Specific legislative measures, such as the Freedom of Information Act (P.L. 90–23, 5 U.S.C. 522, as amended) and the Privacy Act of 1974 (P.L. 93–579, 5 U.SC 522a), have provided the public with an opportunity to gain access to Government information. To some extent these laws have contributed towards involving the public in the oversight function.

The Freedom of Information Act, enacted in 1966 and amended in 1974, provides that records of Federal Government agencies shall be made available to members of the public and outlines the procedures which private citizens may secure these records.[181] The Act was amended in 1974 after congressional hearings indicated some of the difficulties and delays encountered in obtaining information from Federal agencies. The amended law strengthens specific procedures and practices.

---

[180] See prior section on the implications of surveillance technology for illustration and discussion of the variety of foundations for Federal court decisions.

[181] For a brief review of the Freedom of Information Act developments, see Harold Relyea. Opening government to public scrutiny: a decade of Federal efforts. Public administration review, v. 35. Jan./Feb. 1975.

Overriding a Presidential veto Congress enacted the following amendments that would permit access to information held by Federal agencies:

Requiring the formulation of indices concerning records properly recoverable under the Act;

Redefining the degree of "identification" required of records requested from an agency;

Setting definite time limits for agency response regarding disclosure;

Granting attorney's fees and court costs for successful litigants under the Act;

Providing for *in camera* review of the classification of all agency records;

Requiring annual reports to be submitted to Congress relative to agency compliance with the provisions of the Act Amendments (P.L. 93–502).

Although these amendments to the act have contributed to further dissemination of Government information, public access, of course, is not complete. Some important exemptions to the Freedom of Information Act include:

National defense or foreign policy information that is properly classified;

Material specifically exempted from disclosure by another Federal statute;

Inter-agency or intra-agency memoranda of an advisory nature that would not be available by law other than one agency in litigation with another;

Personnel, medical, and other files that, if disclosed, would be considered an unwarranted invasion of personal privacy;

Investigatory files, but only to the extent that one or more of six specified forms of harm would result; and

Bank records.

Despite these exemptions, an expanded quantity of Government data and information has become available to the public.[182] Furthermore, the Freedom of Information Act, subsequent revelations and court suits have served as important ingredients in halting certain surveillance operations, such as the FBI surveillance of the Socialist Workers Party (SWP).[183] In addition to the Federal statute, a number of States have comparable legislation.

Four other statutes specifically provide access to records, limit disclosure, and provide some safeguards in protecting privacy:

Fair Credit Reporting Act of 1970 (Public Law 93–321; 15 U.S.C. 1681 *et seq.*) regulates consumer and investigative consumer reports and collectors and users of the reports. Provides consumer protections and procedures for correcting or disputing material in the report;

---

[182] For a review of the impact, see Harold Relyea, The administration of the Freedom of Information Act . . . op. cit. A series of articles by George Lardner, Jr. in the Washington Post provided some interesting observations and surveys of FOIA impacts and developments, Washington Post, July 25–July 29, 1976 (Section A).

[183] Recent revelations indicated that FBI surveillance commenced 38 years ago and was terminated in early September of 1976. The SWP has filed a $40 million law suit against the FBI and others associated with the surveillance, which involved electronic bugging and mail covers, infiltration and harrassment.

Crime Control Act of 1973 (Public Law 93–83; 42 U.S.C. 3771) limits the use of criminal history files which contain identification information and arrest, court disposition, appeals, and custody data. Subject access and procedures for correction provided. However, investigative files are exempt from the Act's provisions;

The Family Educational Rights and Privacy Act of 1974 (P.L. 93–380; 20 U.S.C. 1232g) regulates school records of all educational institutions receiving Federal funds. Parents or the pupil have a right to see the information collected on the pupil and to object to the accuracy and dissemination of information about him. In addition, all instructional material used in connection with any research or experimentation program must be available for inspection by parents. Enforcement is through administrative proceedings in which HEW may cut off Federal funds to schools in noncompliance with the Act;

The Privacy Act of 1974 (Public Law 93–579; 5 U.S.C. 552a) gives each record subject a right of access to his records held by Federal agencies. The agencies must specify in the Federal Register all the uses to which they put personal records. An accounting for all disclosures must be maintained for 5 years or the life of the record, whichever is longer. In addition, agencies must generally have the consent of the individual before disclosing his record to those who do not have a "right to know" as part of their work. Certain exemptions to access are made for classified or law enforcement files but not from the public notice requirement.

Agencies may maintain only such personal information as is "relevant and necessary" to the purposes of the agencies and they may not maintain information on religious and political activities unless authorized by statute or by the individual or unless within the scope of law enforcement activity. The Act also restricts the sale or rental of mailing lists and the use of the social security number.

The Privacy Act, however, contains certain important exemptions, both of a general nature (e.g. CIA maintained systems of records) and of a specific nature (e.g. investigatory material compiled for law enforcement purposes and maintained in connection with providing protective services for the President and others).

The recently enacted Government in the Sunshine Act (P.L. 94–409) provided that all multi-headed Federal agencies conduct their business regularly in public session. This theme is muted in terms of surveillance technology awareness, however, since exemptions from the requirement provide for closed meetings for ten specified purposes:

(1) national defense, foreign policy or matters classified by executive order;

(2) agency personnel rules and practices;

(3) information required by other laws to be kept confidential;

(4) trade secrets or financial or commercial information obtained under a pledge of confidentiality;

(5) accusation of a crime or formal censure;

(6) information whose disclosure would constitute an unwarranted invasion of personal privacy;

(7) certain law enforcement investigatory records;

(8) bank examination records and similar financial audits;

(9) information whose premature disclosure could lead to significant financial speculation, endanger the stability of a financial institution or frustrate a proposed agency action;

(10) the agency's involvement in federal or state civil actions or similar legal proceedings where there was a public record.

The Foreign Intelligence Surveillance Act of 1976 (S. 3197), which has been discussed in the previous section at length, is an attempt to curtail warrantless electronic surveillance for foreign intelligence purposes and is designed to modify the Omnibus Crime Control Act exceptions for Presidential authorization for "national security purposes." A series of bills has been introduced in the House of Representatives in the 94th Congress to control electronic surveillance (H.R. 1603), prohibit illegal surveillance of citizens by civil officers of the United States (H.R. 1864), provide new standards and criteria for surveillance practices and procedures (H.R. 141), prohibit military surveillance of civilians (H.R. 142, H.R. 266, H.R. 539), and obtain the consent of all parties affected by the interception of oral communications (H.R. 171, H.R. 620).

The range of legislation and proposals testifies to the variety of circumstances and requirements associated with control of surveillance technology. It further exemplifies the wide-ranging concern with the phenomenon.

3. Congressional Oversight

Over the years Congress has expressed concern with surveillance activities that would infringe on personal freedom and permit the unwarranted examinations and investigations. This interest and concern is reflected in both legislative remedies and congressional hearings and debate on this subject. Chapter III provides illustration and further analysis of the concern with surveillance technology and related subjects. Congress has recognized the need to place additional restrictions on government surveillance. Somewhat paradoxically, while reflecting concern with surveillance operations and activities, Congress has contributed to an expansion in data and information collection through increased requirements for reporting and disclosure. The complexity of society and the demands for greater service and information has encouraged the collection and dissemination of vast amounts of information. Therefore in the last twenty-five years there has been a significant increase in reporting requirements with an important growth in the collection of data by Bureau of the Census, Internal Revenue Service, Department of Health, Education, and Welfare and Civil Service Commission, to name a few.

Congressional oversight of surveillance technology has been dispersed among numerous committees and subcommittees and discussed at length in Chapter III. It suffices to mention at this point some of the ingredients of that dispersal.

Because of the multiplicity of agencies engaged in surveillance, numerous committees possess jurisdiction over its manifestations. Oversight is also possible through the appropriations process and through related issues, such as protection of the constitutional rights of citizens and investigations of alleged abuses of authority. Congress has available support through its staff and affiliated agencies—the Congres-

sional Budget Office, Congressional Research Service, General Accounting Office, and Office of Technology Assessment.[184]

Despite these authorities and support services, congressional oversight of an important user and developer of surveillance technology, the intelligence community, has been characterized as "sporadic, unsystematic, incomplete, and at times casual . . . If this is so, Congress is susceptible to manipulation by the executive branch."[185] Other sources have confirmed this interpretation. The President's Commission on CIA Activities noted that "some improvement in the congressional oversight system would be helpful."[186] The Senate select committee on intelligence, which had been one of the more critical oversight instruments, concluded less charitably:

> Congress, which has the authority to place restraints on domestic intelligence activities through legislation, appropriations, and oversight committees, has not effectively asserted its responsibilities until recently. It has failed to define the scope of domestic intelligence activities or intelligence collection techniques, to uncover excesses, or to propose legislative solutions. Some of its members have failed to object to improper activities of which they were aware and have prodded agencies into questionable activities.[187]

Despite these findings, the creation of a permanent Senate Select Committee on Intelligence may continue the intensive investigations and oversight initially raised by the House and Senate select committee on intelligence. Other legislative innovations which improve oversight capabilities over intelligence and surveillance practices have included expanding senatorial confirmation requirements for intelligence and law enforcement officials, limiting tenure for those officials, independent funding of the Intelligence Community Staff, requesting frequent testimony from agency officials, and increasing requests to the General Accounting Office and the Congressional Research Service.

4. Federal Commission Studies

Another element in control and oversight of surveillance technology are the Federal commissions designed to study and recommend certain practices, operations, activities, and statutes. The single most relevant example has been the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. (The Commission's summary conclusions and recommendations, released in 1976, are included in Chapter IV. B.) Created by Title III of the 1968 Omnibus Crime Control Act (18 U.S.C. 2510–2520), the National Wiretap Commission was authorized "to conduct a comprehensive study and review of the operation of Title III in the first six years after its enactment."[188]

Of import has been the June 1976 report of the U.S. Privacy Protection Study Commission entitled "Federal Tax Return Confidential-

---

[184] A review of congressional oversight of intelligence, which has many of the elements associated with oversight of surveillance technology, is provided in a report in Chapter III. B. 3. U.S. Library of Congress. Congressional Research Service. Congressional oversight of intelligence: status and recommendations. Multilith prepared by Frederick M. Kaiser. March 11, 1976.

[185] Harry Howe Ransom. Congress and the intelligence agencies. In Harvey C. Mansfield (ed.). Congress against the President. Proceedings of the Academy of Political Science, v. 32, n. 1, 1975, p. 159.

[186] U.S. President's Commission on CIA Activities within the United States. op. cit., p. 14.

[187] U.S. Congress. Senate, Select Committee to Study . . . op. cit., p. 277.

[188] U.S. National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. Op. cit., pp. xi–xix.

ity" and dealing with the disclosure policies of the Internal Revenue Service.[189] During the early 1970's, the National Advisory Commission on Criminal Justice Standards and Goals issued a series of reports, conclusions, and recommendations relating to certain surveillance practices and technologies.[190]

Another illustration of the sundry commissions which have dealt with aspects of surveillance technology is the President's Commission on the Assassination of President John F. Kennedy.[191] The findings, conclusions, and recommendations provided a basis for expanded authority of the Secret Service to request the support and assistance of and to improve communications with other Federal agencies. As a result, the surveillance capability of the National Security Agency was made available to the Secret Service and it gained greater access to certain FBI records. Finally, the efforts of the Commission on CIA Activities within the United States[192] provides extensive review of CIA surveillance operations and use of appropriate technology domestically.

5. Executive Branch Oversight and Controls

The executive branch, including the President as well as agency, department, and bureau officials, have impressive oversight responsibilities. In essence, they are responsible for the daily execution and implementation of policy, developing relevant guidelines and criteria, and insuring the protection of citizen rights and liberties. With regard to control and accountability of the utilization of surveillance technology by, at least, intelligence agencies, the executive branch has been deficient, according to the Senate select committee on intelligence.[193]

That shared failure is summarized as follows by the Select committee:

> The Committee finds that those responsible for overseeing, supervising, and controlling domestic activities of the intelligence community, although often unaware of details of the excesses described in this report, made those excesses possible by delegating broad authority without establishing adequate guidelines and procedural checks; by failing to monitor and coordinate sufficiently the activities of the agencies under their charge; by failing to inquire further after receiving indications that improper activities may have been occurring; by exhibiting a reluctance to know about secret details of programs; and sometimes by requesting intelligence agencies to engage in questionable practices. On numerous occasions, intelligence agencies have, by concealment, misrepresentation, or partial disclosure, hidden improper activities from those to whom they owed a duty of disclosure. But such deceit and the improper practices which it concealed would not have been possible to such a degree if senior officials of the Executive Branch and Congress had clearly allocated responsibility and imposed requirements for reporting and obtaining prior approval for activities, and had insisted on adherence to those requirements.

---

[189] U.S. Privacy Protection Study Commission. Federal tax return confidentiality. Washington, D.C., U.S. Govt. Print. Off., 1976.

[190] U.S. National Advisory Commission on Criminal Justice Standards and Goals. A national strategy to reduce crime; Report on the criminal justice system; and Report on police. Washington, D.C., U.S. Govt. Print. Off., 1973.

[191] U.S. President's Commission on the Assassination of President John F. Kennedy. Report. Washington, D.C., U.S. Govt. Print. Off., 1964.

[192] U.S. Commission on CIA Activities within the United States. Report. Washington, D.C., U.S. Govt. Print. Off., 1975. Yet another commission, the National Commission on Individual Rights, was created by Congress (P.L. 91-452) with responsibility to examine wiretapping and electronic surveillance, among other items. However, the President had failed to appoint its public members and the Commission was unable to meet.

[193] U.S. Congress. Senate. Select Committee to Study Government Operations . . . Final Report, Book II. Op. cit.

Subfindings

(a) Presidents have given intelligence agencies firm orders to collect information concerning "subversive activities" of American citizens, but have failed until recently to define the limits of domestic intelligence, to provide safeguards for the rights of American citizens, or to coordinate and control the ever-expanding intelligence efforts by an increasing number of agencies.

(b) Attorneys General have permitted and even encouraged the FBI to engage in domestic intelligence activities and to use a wide range of intrusive investigative techniques—such as wiretaps, microphones, and informants—but have failed until recently to supervise or establish limits on these activities or techniques by issuing adequate safeguards, guidelines, or procedures for review.

(c) Presidents, White House officials, and Attorneys General have requested and received domestic political intelligence, thereby contributing to and profiting from the abuses of domestic intelligence and setting a bad example for their subordinates.

(d) Presidents, Attorneys General, and other Cabinet officers have neglected until recently to make inquiries in the face of clear indications that intelligence agencies were engaging in improper domestic activities. . . .

* * * * * * *

(f) Intelligence agencies have often undertaken programs without authorization with insufficient authorization, or in disregard of express orders.

(g) The weakness of the system of accountability and control can be seen in the fact that many illegal or abusive domestic intelligence operations were terminated only after they had been exposed or threatened with exposure by Congress or the news media. [194]

Recent recommendations for improved executive accountability and control have resulted in the creation of the Intelligence Oversight Board, a three-member commission composed of private citizens to monitor the intelligence community and to report to the President; an expansion of the President's Foreign Intelligence Advisory Board from ten to seventeen members; and certain reorganizations of the intelligence agencies and control structures.

Further executive branch involvement regarding controls and oversight is evident in newly devised guidelines issued by the Attorney General surrounding FBI investigations and the series of proposed standards and guidelines developed by the Law Enforcement Assistance Administration, which were examined in detail in the previous section on policy and implications.

Finally, internal departmental and agency control can be effected through offices of inspector general and offices of audit and investigation in appropriate departments and agencies. The Department of Justice Office of Professional Responsibility and the Criminal Division Public Integrity Unit are example of such offices. The Civil Rights Division of the Justice Department has been engaged in the investigation of alleged misconduct regarding the FBI's counterintelligence and infiltration programs and consequently serves as a departmental overseer. Furthermore, Attorney General Levi created a temporary three-member unit on April 5, 1976 to assist him in monitoring the implemention of the Justice Department guidelines relating to FBI investigations.

As implied in these descriptions, offices which possess some internal investigative and monitoring function, vary dramatically in their authority, resources, responsibilities, and duties. In contrast to the limited, temporary structure created by the Attorney General to monitor the new guidelines, the House Select Committee on Intelli-

[194] Ibid., pp. 265–266.

gence recommended a permanent, statutorily-created Inspector General for Intelligence with impressive authorities and access:

INSPECTOR GENERAL FOR INTELLIGENCE

1. The select committee recommends the establishment of an independent Office of the Inspector General for Intelligence, who shall have full authority to investigate any possible or potential misconduct on the part of the various intelligence agencies or the personnel therein. The IGI shall be appointed by the President, with the approval of the Senate, for a term of 10 years and shall not be permitted to succeed himself. The IGI shall have full access on demand to all records and personnel of the intelligence agencies for the purpose of pursuing his investigations. He shall make an annual report to the Congress of his activities and make such additional reports to the intelligence committees or other appropriate oversight committee as he may choose or the committee may direct.[195]

F. Summary and Conclusions

Surveillance technology and its development and utilization have become enmeshed with the concerns over abuses and misuses of this potent attribute of modern society. Despite the recent nature of specific problems and manifestations of surveillance technology, the underlying apprehensions have a lengthy heritage in the American democratic system. The potentially competing requirements of domestic and national security juxtaposed with civil liberties and constitutional rights have been recognized by numerous observers and practitioners of politics throughout the history of the United States. James Madison designated a dual responsibility for democracy—to enable Government to control the governed and oblige Government to control itself.[195a] John Adams' apprehensive warning elaborates on a similar theme—"Remember, democracy never lasts long. It soon wastes, exhausts, and murders itself. There was never a democracy which did not yet commit suicide." [196] In another era and under different conditions, Abraham Lincoln questioned whether a Government must be too strong for its citizens' liberties or too weak to maintain its own existence. These parallel concerns, fostered in the apocalyptic periods of the Revolution, Constitution building, and Civil War, are no less meaningful with regard to surveillance technology in the contemporary era than they were in other periods of American history.

Writing in *The New Utopians*, Robert Bougslaw applies the concern to contemporary society:

Our own utopian renaissance receives its impetus from a desire to extend the mastery of man over nature. Its greatest vigor stems from a dissatisfaction with the limitations of man's existing control over his physical environment. Its greatest threat consists precisely in its potential as a means for extending the control of man over man.[197]

Surveillance technology has become a valuable mechanism in intelligence gathering, law enforcement, and national security. Yet, it is that vast capability and expanded scope and magnitude coupled with

---

[195] U.S. Congress. House of Representatives. Select Committee on Intelligence. Recommendations of the final report. 94th Congress, 2d session. Feb. 11, 1976. House Report No. 94–833.

[195a] Note 178, supra.

[196] John Adams quoted in Alpheus Thomas Mason, America's political heritage: revolution and free government—a bicentennial tribute. Political science quarterly, v. 91, Summer 1976. P. 203.

[197] Robert Bougslaw. The New Utopian: A study of system design and social change. Prentice-Hall, Inc. Englewood Cliffs, N.J., 1965. P. 204.

the increasingly sophisticated and commonplace surveillance equipment which elicit apprehension.

What measurements exist are staggering—3.8 billion records (on individuals) held by 85 separate Federal departments or agencies; more than 80 police or investigative units in addition to more than 30 intelligence units; millions of dollars provided for electronic surveillance equipment by one agency (LEAA) to State and local government units; substantial military and civilian Research and Development efforts; extensive training programs existing throughout the Federal Government; and required support and extensive assistance from private firms engaged in national and international communication. In combination with this utilization is a technology whose quantitative and qualitative developments may supersede existing authorities and standards and make obsolete controlling statutes and judicial interpretations. Polygraphs, visual surveillance mechanisms, electronic eavesdropping equipment, and computerized records systems illustrate the range of covert and overt and passive and active surveillance technologies. These devices combine with modern technological characteristics, such as miniaturization, modularity, and improved quality, to make available a surveillance technology which is highly intrusive yet, at the same time, increasingly less detectable.

Under these conditions, even legitimate use of surveillance technology may well infringe on the civil liberties of individuals. The impossibility of absolute protections are implicit in the "minimization" provisions included in legislative proposals and administrative standards, which attempt to limit the invasion of innocent parties' privacy. The intrusive nature of surveillance technology, both covert and overt, makes tenuous the constitutional protections afforded to U.S. citizens as well as to foreign nationals in the United States.

Restrictions on legislative and judicial controls inherent in "executive privilege" and unwarranted, nonconsensual surveillance for "national security" purposes provide further anxiety regarding the protection of individual liberties.

The excessive use of highly intrusive surveillance technologies along with abuses of relevant authority have been principal revelations of the congressional investigations of intelligence activities. These conclusions reveal an absence of centralized decision-making and serious weaknesses in control and accountability to elected Government officials. Moreover, the infringement of the right of privacy and of those articulated in the First, Fourth, and Fifth Amendments to the Constitution reaches serious proportions under such conditions. Even those not directly involved may experience a "chilling effect" on their own political rights and civil liberties.

Finally, consideration must be given to the unintended consequences and latent functions of surveillance. Whether in law enforcement or intelligence production, surveillance serves as a threshold activity, as a precondition to other activity and not necessarily just for its own sake. Consequently, some surveillance technology may serve as a stimulant or catalyst to additional or different forms of surveillance. Surveillance technology may also encourage intervention or an attempt to manipulate events as well as a tendency to misuse the surveillance product. Possible examples of these latent functions include:

The surreptitious and possibly illegal entries conducted by the FBI to gather information and to install electronic surveillance devices; [198]

COINTELPRO, the FBI's counter-intelligence program of domestic covert action, which included and utilized supposedly confidential income tax information and illegal or improper surveillance techniques, as part of a program to discredit certain groups and disrupt their activities; [199]

The FBI's attempt to "neutralize" Dr. Martin Luther King, Jr. as a civil rights leader through discrediting and involving electronic eavesdropping; [200]

"Operations CHAOS," the CIA's operation ostensibly designed "to determine foreign contacts with American dissident groups . . . (which) resulted in the accumulation of considerable material on domestic dissidents and their activities . . . and which employed various surveillance techniques"; [201] and

The Special Service Staff of the IRS, which existed from 1969 to 1973 and served as a political intelligence arm of the IRS, utilized by the White House in acquiring confidential tax information on individuals on its "enemies list," involving operations described as "a dangerous abuse of the enormous power . . . (of) the tax collection arm of government." [202]

Since this overview and report have concentrated on Federal Government involvement in surveillance technology, there has been little discussion of State and local government and the private sector. The invasion of constitutional rights is a likely consequence of surveillance technology in these other spheres and demands the inspection this report is unable to provide.

The weakness or absence of measurements of even Federal involvement has not precluded some major interpretations of Federal policy in this area. Given the dispersed and diffused policy-making system; the independence and multiplicity of agencies utilizing, developing, and supporting surveillance technology; and the absence of comprehensive legislative and administrative standards and guidelines, surveillance technology is determined by a series of policies rather than a coherent policy. Beyond this, various statutory exemptions, Executive powers (e.g., "executive privilege" and an espoused "inherent" power to conduct unwarranted surveillance), the absence of centralized policy-making, innovative technologies, the increased availability and limited detectability of contemporary technologies, and the clandestine or covert nature of much surveillance combine to produce a policy sphere which may circumvent the usual channels of control and accountability in a democracy.

A series of abuses, misuses, and problems associated with surveillance technology, noted in the previous sections, confirms this interpretation:

---

[198] U.S. Congress. Senate. Select Committee to Study Governmental Operations . . . Final Report Book II. Op. cit., p. 61.
[199] Ibid., pp. 10–11.
[200] Ibid., p. 11.
[201] President's Commission on CIA Activities within the United States. Op. cit., p. 130.
[202] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Political intelligence in the Internal Revenue Service: the Special Service Staff. A documentary analysis prepared by the staff of the Subcommittee. 93d Congress, 2d session. Dec. 1974 (At head of title—Committee Print.) p. iv.

Unauthorized and/or illegal surveillance;

Excessive use of particular technologies, especially the highly intrusive and convert;

Surveillance devices and equipment which are unaccounted for;

Misleading estimates of certain costs and expenditures;

Misleading estimates of utilization;

Manipulation and imprecision of concepts to justify surveillance technology use;

Absence of certain safeguards of computerized personal records systems;

Political abuse of computerized personal records systems;

Excessive overhearing of innocent parties' communications;

Inadequate controls over dissemination of the surveillance product;

A lack of clarity or detail and/or an absence of standards and guidelines in some instances; and

Improper use of surveillance technology and its product, serving as an ingredient in counter-intelligence operations, activities designed to descredit individuals, and/or intimidation or harrassment of individuals and groups.

These findings, based on an examination of Federal Government involvement in surveillance technology, do not necessarily argue inviolably against surveillance technology, which has valuable functions for a society and will remain. The findings do, however, present strong evidence for circumscribing the use of surveillance technology, limiting its authorization, providing greater coherence and standardization of use, and insuring adequate and extensive controls and oversight. The conditions surrounding Federal involvement and the characteristics of contemporary surveillance technology strongly suggest that these objectives are possibly elusive and perplexing. Certainly they will be difficult to achieve and demand a high degree of commitment, integrity, and support from the overseers as well as the practitioners. In light of these objectives and the broad ramifications of surveillance technology, the dangers inherent in uncontrolled use, and the state of knowledge about Federal utilization and support, this chapter concludes with a series of suggestions for further congressional consideration, some of which are adopted from the sources used in this analysis:

- Creation of a legislative task force, possibly staffed by committee staff and personnel of the Congressional support agencies—Congressional Budget Office (CBO), Congressional Research Service (CSR), General Accounting Office, (GAO), and Office of Technology Assessment (OTA)—to provide a comprehensive and detailed examination of surveillance technology, especially with regard to Federal involvement. Related avenues of inquiry might include the contributions from the private sector as they affect national policy, particularly with consideration to research and development and direct assistance in the Federal Government efforts. Such an analysis might include examination of the role of multinational corporations in such assistance in surveillance abroad and the contracting policies of relevant agencies (e.g., contracting to foreign-based firms, to multi-national corporations, and to domestic firms);

- Increased utilization of congressional support agencies for continual monitoring of state of the art and applications of surveillance technology, including improved and increased GAO access to and auditing of relevant intelligence and law enforcement utilization, jointly conducted program evaluations and cost-effectiveness analyses, OTA assessment of proposed technological innovations and potentialities of certain technology proposals;
- Increased congressional oversight, involving more regularized and systematized efforts, coordination among appropriate committees and subcommittees, and possible re-structuring in the House of Representatives to parallel the Senate Select Committee on Intelligence;
- Strengthened or re-structured Executive oversight mechanisms, including a comprehensive statutory office of inspector general and internal investigation;
- Clearer and more stringent legislation and administrative sanctions dealing with improper or illegal utilization of surviellance technology;
- Clarification of administrative responsibility within an agency for custody and the use of certain surveillance equipment and for the utilization of surveillance technologies;
- Improved disclosure mechanisms for the use of particular technologies;
- Clearer and more definitive standards and guidelines for surveillance technology utilization, including the use of questionable techniques and technologies, the dissemination of information, and the safeguarding of computerized record systems;
- Statutory clarification and restrictions of Presidential discretion with regard to authorization or conducting surveillance for national security purposes and/or foreign intelligence purposes;
- Statutory clarification and limitations on the surveillance conducted by law enforcement and intelligence agencies involving United States citizens and aliens in the United States and U.S. citizens abroad;
- Statutory restrictions and subsequent penalties for misuse of surveillance systems and products;
- Expanded reporting requirements to the judiciary (and eventually the Congress) for court-authorized interception of oral and wire communications;
- Development of parallel reporting requirements to appropriate congressional committees for unwarranted interceptions.

CHAPTER II

Significant Developments

*A. Chronology of Technological Developments**

Modern surveillance equipment reflects the advanced state-of-the-art in the field of electronics, including successful miniaturization of components and development of new technologies for the transmission of information. These technologies encompass such innovations as: microform products, computer storage of vast data bases, and advancements in laser transmission. The evolution of the electronics industry laid the foundation for many of the modern surveillance devices.

In addition to the actual equipment innovations, it is important to view these inventions within the context of their impact upon society. This impact came as refinements to existing techniques led to greater public access and proliferation of devices. Below is a chronological outline of the major discoveries in the field of electronics which have contributed to the scope and variety of surveillance techniques available today.

1800's

During the industrial revolution of the 19th century, major technological advances were made in several key areas. It was during this period that the first concepts for computer design were advanced by Charles Babbage. In the latter part of the century critical achievements occurred in wireless and voice communication. Concurrently, George Eastman produced practical photographic film, thereby giving impetus to a widespread public interest in photography.

1820–35—Charles Babbage outlines designs for first computers.

1844—Samuel F. B. Morse sends first public telegraph message.

1858—First trans-Atlantic cable is laid.

1876—Alexander Graham Bell invents the telephone.

1879—Sir William Crookes conducts early experiments leading to discovery of cathode-rays.

1884—Herman Hollerith of the U.S. Census Bureau develops tabulating machine for use with punched cards to facilitate 1890 Census.

1889—George Eastman develops a practical photographic film.

1892—Telephone connection between Chicago and New York is established.

1899—1901—Guglielmo Marconi transmits first telegram across English Channel—first trans-Atlantic wireless message is sent.

Early 1900's

The impact of these core inventions were not fully realized until their mass production could be accomplished through standardized

*This section was prepared by Jane B. Staenberg, Analyst in Information Sciences, Congressional Research Service, Library of Congress. The information for this chronology was supplied by several encyclopedias of science and technology, histories of the electronics industry, and chronologies of major scientific discoveries.

industrial production methods. Major companies in the field of electronics made great strides during this period both in improving existing tools and man-machine techniques and marketing such products to the public.

1920's—Industrial research into television and the introduction of sound films leads to major improvements in photo electric devices.

1921—"Radio Corporation of America" (RCA) established, combining the vacuum tube and related circuitry patents of Marconi, Bell Telephone, General Electric, Westinghouse and Armstrong.

1925–30—Industry begins to manufacture complete radio receivers. Transmitters capable of handling greater power are produced.

World War II

World War II provided the impetus for rapid advancements in the field of electronics. Heavily funded military applications provided a testing ground for many technical breakthroughs. Wartime requirements led to a broad spectrum of improvements in voice transmission, portable monitoring equipment, and improved surveillance techniques. Government support was coupled with an increased commitment on the part of industry to produce rapid advances.

1940's—Development of radar by the British. Development of portable transceivers ("walkie-talkies") and mobile transmitters in cars.

1940–45—Tape recorder equipment built with improved sound quality.

1943—Howard Aiken demonstrates the first operational program-controlled computer in the U.S.

Post-War Development

Following World War II, computer development moved forward on a broad front. While the initial steps had been taken during the war, significant continued Government support allowed computer technology to develop into a major industry. At the same time, improvements continued in the areas of miniaturization, storage options, and the portability of equipment.

1943–49—Individual organizations, universities, and Federal Government laboratories pioneer in electronic computing and other forms of data processing.

1947–55—Small new enterprises with highly skilled people form to develop computer and related communications technology (with heavy Government R & D sponsorship)—"first-generation" hardware becomes broadly utilized.

1948—Physicists at the Bell Laboratories invent the transistor. Equipment increasingly more efficient, lighter, portable, and able to run cooler—a major step in process of miniturization.

1950's—Transistors improved and prices reduced. Tape recorder equipment improved and prices reduced.

1955–64—Large organizations manufacturing computers educate customers on a broad scale in the use of computer technology, utilizing "second-generation" hardware.

1958—Lasers invented by A. Schawlow and C. H. Townes. Development enables optical frequencies to be used as exactly defined carrier frequencies for communications channels.

1960's to Present

In an era which has featured the refinement of existing technologies, the past 15 years have provided a stage for milestone advancements in diversified computer operations and the transmission of information on a global scale. "Third-generation" equipment was developed in the computer industry, providing increased capabilities for information storage, processing, and retrieval. Currently, the production of microprocessors permits greatly improved communications networks, while satellites placed in orbit allow us to provide new services to specific geographic areas and send signals around the world. These innovations have had a significant impact on the ability to gather (or intercept) information on a large scale and transmit it great distances.

1960's—Development of the integrated circuit, making extremely small components possible. Printed circuit techniques make production less expensive through batch production.

Microfiche technology becomes a practicality.

Communications satellites placed in orbit allow the relaying of signals around the world.

Time-sharing and network systems provide the capability of interacting between remote consoles and a central computer, providing instantaneous feedback and access to multiple data bases.

1963–69—Computer customers acquire growing sophistication, and begin to influence the direction of new product developments—enter "third-generation" systems.

1965—Audio cassettes of tapes initiated providing automatic winding and easy use.

Video recorders gain wider use. No longer necessary to wait for development of film.

1970's—Standardization of computer products continues with periodic improvements in computer systems. Steady growth in computer services and support products.

1974—Microprocessors go into quantity production. Field tests are done on millimeter wave-guide system that can carry 230,000 simultaneous conversations.

1975—Video record players are perfected.

1976—Continued developments in the area of semiconductor devices make possible powerful computers in new forms.

Improvement in long-distance communications continues with developments in the areas of optical fibers and solid state lasers.

*B. Chronology of Administrative and Legislative Initiatives**

This chronology examines some of the major administrative and legislative developments regarding surveillance technology. The focus is on the creation of executive agencies which have made substantial use of surveillance technology and on congressional controls (via legislation) over such agencies and the utilization of surveillance technology. However, there is not space to list all the Federal executive agencies which have an intelligence or law enforcement function and possess

*Chronology prepared by John Ridley, Analyst in American Government. Congressional Research Service, Library of Congress.

investigative authority and intelligence capabilities. Consequently, only the major intelligence/law enforcement agencies are included in the chronology.

1882—Office of Naval Intelligence created.

1908—Attorney General Charter Bonaparte created, via internal memorandum, the Bureau of Investigation.

1917—Secretary of War Newton Baker created the first Division of Military Intelligence in the Department of the Army.

1924—J. Edgar Hoover named head of the Bureau of Investigation of the Justice Department.

1934—Congress passed the Federal Communications Act. Section 605 of the act forbade interception and divulgence of telephone and radio messages.

1936—President Roosevelt requested intelligence information on domestic subversive activities via the Secretary of State and the Attorney General from the Federal Bureau of Investigation.

1941—President Roosevelt created the Office of Strategic Services to collect and analyze strategic information for the use of the Joint Chiefs of Staff during WWII. (7 F.R. 4469–4470)

1946—President Truman established the National Intelligence Authority with a support staff called the Central Intelligence Group. (11 F.R. 1337, 1339)

1947—Enactment of the National Security Act, establishing the CIA, NSC and the basic modern U.S. intelligence establishment. (P.L. 80–253, 5 U.S.C 172)

1949—Central Intelligence Agency Act of 1949 further delineated the functions of the CIA, which had been established pursuant to the National Security Act of 1947. (P.L. 81–110, 50 U.S.C. 403a–j)

1950—The IAC or Intelligence Advisory Committee created as an interdepartmental coordinating committee for intelligence. Later changed name to the United States Intelligence Board (USIB).

1952—The National Security Agency was established by secret Presidential directive as a separate agency within the Department of Defense.

1955—Hoover Commission Task Force on Intelligence issued a report recommending creation of the President's Foreign Intelligence Advisory Board (PFIAB).

1955—President Eisenhower appointed PFIAB [President's Foreign Intelligence Advisory Board] (Executive Order No. 10656) to give the President independent evaluations of the intelligence community.

1961—Creation of the Defense Intelligence Agency (DIA) for the purpose of unifying military intelligence efforts.

1968—Congress enacted the Omnibus Crime Control Act of 1968, which among other things established guidelines for wiretapping and electronic surveillance. The Act also created the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. (P.L. 90–351)

1970—Congress passed the Fair Credit Reporting Act of 1970 which included provisions to require consumer reporting agencies to adopt procedures to insure the confidentiality, accuracy, relevancy, and proper utilization of credit report information. Consumer access to the

information and provisions governing disclosure of such information were inclusions. (P.L. 91–508)

1971—Creation of Intelligence Resource Advisory Board (IRAB) for purposes of better managerial control of the intelligence community's budget.

1973–74—Senate Watergate Committee conducted investigation into the conduct of the 1972 Presidential campaign which touched on possible illicit CIA activity and White House surveillance activities.

1974—Creation of the National Commission on Electronic Fund Transfers by the Congress. Commission functions include conducting a thorough study and investigation and recommend appropriate adminstrative action and legislation necessary in connection with the possible development of public or private electronic fund transfer systems. with concern for consumer rights to privacy and confidentiality and the implications of such a system expanding internationally and into other forms of electronic communications. (P.L. 93–495)

1974—The Privacy Act of 1974 granted each record subject a right of access to his records held by Federal agencies and created the Privacy Protection Study Commission. (P.L. 93–579; 55 U.S.C. 552a)

1975—Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activity established pursuant to S. Res. 21.

1975—Creation of House Select Committee on Intelligence pursuant to H. Res 138 and H. Res. 591.

1975—President Ford created the Commission on CIA Activities to evaluate domestic activities of the CIA. (E.O. 11828)

1976—Establishment of the permanent Select Committee on Intelligence (to oversee the intelligence community) by the U.S. Senate. (S. Res. 400)

CHAPTER III

Congressional Action and Reaction

*A. Review of Selected Congressional Hearings and Studies**

In recent years a substantial part of congressional concern and interest in surveillance technology has focused on some of the technological innovations which may be used to invade personal privacy and permit unwarranted surveillance of individuals and groups. That concern has extended to the application of certain surveillance technologies and techniques, the authorities under which such practices occur, and the possible misuse of these authorities and technologies.

Over the past two decades there has been a growing concern that the use of warrantless wiretapping, eavesdropping, and other surveillance techniques would contribute to the erosion of personal freedoms and civil liberties. It is argued, for instance, that widespread surveillance, especially that conducted by the Government, may have a serious "chilling effect" on the economic, social, and political activities of individuals and organizations.[1] Furthermore, congressional investigations have discovered a number of improprieties, abuses, or hazards associated with the use of surveillance technology. These include the findings that certain Federal agencies have engaged in surveillance or utilized certain surveillance technologies without proper authorization; that there is an absence of legislation governing the use of particular types of surveillance technologies and the agencies which are the principal users of such technology; that the increasingly sophisticated technologies of surveillance may circumvent legislation or controls designed to govern their operation; that judicial authorization is not a prerequisite for electronic surveillance in cases involving national security; that Presidential authority regarding electronic surveillance for national security purposes has been abused; that there is often a lack of administrative guidelines or standards for the use of surveillance technologies and intelligence collection and dissemination; and that data and information collected is not properly evaluated in all cases and may be unrelated to the jurisdictional responsibilities of the agency, although such information remains in the agency files.

Some congressional hearings and investigative studies have discussed the explicit use of surveillance technology while others have examined related issues. The major subjects have included the following:

electronic surveillance for national security purposes;

Government surveillance of Federal employees;

---

*This section was prepared under the direction of staff of the Senate Subcommittee on Constitutional Rights by Frederick M. Kaiser, Analyst in American National Government, and Louise Giovane Becker, Analyst in Information Sciences, Congressional Research Service, Library of Congress.

[1] "The government's surveillance activities in the aggregate—whether or not expressly intended to do so—tends (sic) . . . to deter the exercise of First Amendment rights by American citizens who became aware of the government's domestic intelligence program." U.S. Congress, Senate, Select Committeee to Study Governmental Operations with Respect to Intelligence Activities. Intelligence activities and the rights of Americans. Final Report, Book II. 94th Congress, 2d session, April 26, 1976, p. 17.

the use of polygraphs in the public and private sector;
proposals for a National Data Bank;
criminal justice information systems;
domestic surveillance by the Department of Defense and other Federal agencies, principally the CIA, NSA, and FBI;
Internal Revenue Service's development of a special surveillance unit, information gathering and retrieval system, and political exploitation of confidential taxpayer records;
and computer security and computer abuse.

Congressional investigations have been undertaken either to examine legislative proposals or to review previous or existing practices regarding surveillance technology. Congressional oversight has occurred primarily in accordance with the mandate of the Legislative Reorganization Act of 1970 (P.L. 91–510). Sec. 118 of the 1970 Act provides that "each committee shall review and study, on a continuing basis, the application, administration, and execution of laws" under its jurisdiction. Congressional oversight of surveillance technology and its implications might also be conducted as part of a specific mandate to a select committee, such as the select committees on intelligence in both chambers; as a by-product of an investigation into related subject matter (e.g. civil liberties and constitutional rights); or as part of the broad responsibilities of the House and Senate Committees on Government Operations relating to the economy and efficiency of Government operations and programs and reorganizations of the executive branch.

Legislative Initiatives

Legislative initiatives undertaken by the Congress in this area have been designed to protect the privacy of the public regarding information collected on individuals and to provide statutory authority and guidelines for certain surveillance technologies. The following represent some of the primary developments in these areas.[2]

(1) The Omnibus Crime Control and Safe Streets Act of 1968 (P.L. 90–351, Title III; 18 U.S.C. 2511 *et seq.*) established prohibitions on interception and disclosure of wire or oral communications by private parties or Government officials without court authorization. However, certain constitutional powers of the President with respect to electronic surveillance for national security purposes were not affected by this legislation. The Omnibus Crime Act also provided for procedures to secure judicial authorization for such interception and authorized, for the first time, the use of intercepted wire or oral communications as evidence in criminal trials.

(2) The Fair Credit Reporting Act of 1970 (P.L. 91–508, Title VI; 15 U.S.C. 1681 *et seq.*) regulates consumer reports (information about bill paying habits) and investigative consumer reports (information relating behavioral traits such as drinking habits). Both collectors (credit agencies) and users of information (e.g., department stores and lenders) are regulated. The consumer has the right to know the nature and sources of the information contained in the files of the consumer reporting agency and procedures are available for correcting or disputing material in the report. Enforcement is by a civil suit

[2] Excerpt for the Omnibus Crime Control Act of 1968, the legislative references and descriptions were prepared by Jerome Hanus, U.S. Library of Congress, Congressional Research Service, Privacy: concepts and problems, Issue Brief number IB74123 by Jerome J. Hanus, March 23, 1976 (Washington, D.C.), 1976, pp. 1–3.

by the consumer and noncompliance with the Act is an unfair trade practice, within the jurisdiction of the FTC.

(3) The Crime Control Act of 1973 (P.L. 93–83; 42 U.S.C. 3771; 40 F.R. 22114 (May 20, 1975)) limits the use of criminal history files which contain identification information and arrest, court disposition, appeals, and custody data. Individuals have opportunity for access to their records and to correct erroneous information. However, investigative files are exempt from the Act's provisions.

(4) The Family Educational Rights and Privacy Act of 1974 (Public Law 93–380; 20 U.S.C. 1232(g) regulates school records of all educational institutions receiving Federal funds. Parents or the pupil have a right to see the information collected on the pupil and to object to the accuracy and dissemination of information about him/her. In addition, all instructional material used in connection with any research or experimentation program must be available for inspection by parents. Enforcement is through administrative proceedings in which HEW may cut off Federal funds to schools in noncompliance with the Act.

(5) The Privacy Act of 1974 (Public Law 93–579; 5 U.S.C. 552(a)) gives each record subject a right of access to his records held by Federal agencies. The agencies must specify in the Federal Register all the uses to which they put personal records. An accounting for all disclosures must be maintained for 5 years or the life of the record, whichever is longer. In addition, agencies must generally have the consent of the individual before disclosing his record to those who do not have a "right to know" as part of their work. Certain exemptions to access are made for classified or law enforcement files but not from the public notice requirement.

Agencies may maintain only such personal information as is "relevant and necessary" to the purposes of the agencies and they may not maintain information on religious and political activities unless authorized by statute or by the individual or unless within the scope of law enforcement activity. The Act also restricts the sale or rental of mailing lists and the use of the social security number.

A significant provision in the Act established for 2 years the Privacy Protection Study Commission, which would study various aspects of privacy in both private and public sectors and is encouraged to prepare model legislation for State and local governments. Mr. David Linowes is the Chairman of the seven-member Commission. As of March, it had held seven meetings, all open to the public. The meetings were organizational in nature but testimony was taken from IRS concerning the use of the income tax return.

Agencies may be liable to civil and criminal penalties for violating the Act. And a predominantly successful plaintiff may be awarded attorney fees and court costs.

The Office of Management and Budget, which has oversight responsibilities under the Act issued its guidelines for implementing the Act on July 9, 1975. The Act itself went into effect on Sept. 27, 1975, and by that date over 8,000 systems of records were noticed in the Federal Register.

Presently, both Chambers are examining bills which are intended to provide certain controls over surveillance technology and intelli-

gence activities. For instance, proposals regarding the Foreign Intelligence Surveillance Act (S. 743, S. 1888, and S. 3197) have elicited hearings by the Criminal Laws and Procedures Subcommittee of the Senate Judiciary Committee [3] and the newly-formed permanent Senate Select Committee on Intelligence. The bills, dealing with electronic surveillance for foreign intelligence and national security purposes, incorporate provisions requiring a judicially approved warrant procedure for the President and his designate and limiting the scope of such surveillance to individuals acting "pursuant to the direction of a foreign power." In the House of Representatives, a series of proposals designed to curtail and control electronic as well as other types of surveillance has been advanced. Hearings have been held by the House Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice with respect to bills requiring new standards and criteria for surveillance practices and procedures (H.R. 141), prohibition of military surveillance of civilians (H.R. 142, H.R. 266, H.R. 539); the consent of all parties affected by the interception of oral communications (H.R. 171, H.R. 620); court orders for the interception of communications, mail openings, inspection of certain records, and entering any residence (H.R. 214, H.R. 414); restrictions on the authorization of electronic surveillance and wiretapping (H.R. 1603); and prohibitions on the illegal surveillance of citizens by civil officers of the United States (H.R. 1864).[4]

In addition to the legislation, approved or contemplated, dealing with surveillance technology, Congress has created Federal study commissions to examine related issues and make recommendations. Among these commissions are the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance (P.L. 90–351), which recently released its final report; [5] the National Commission on Electronic Fund Transfers (P.L. 93–495); the Privacy Protection Study Commission (P.L. 93–579); and the Commission on Federal Paperwork (P.L. 93–556).

Internal congressional reorganizations are a final example of a growing awareness of the issues and problems associated with surveillance technology. The most notable instances in the 94th Congress have been the establishment of select study committees on intelligence in both chambers and the creation of a permanent Select Committee on Intelligence in the Senate. The permanent Senate Select Committee on Intelligence (S. Res. 400, approved May 19, 1976) has extensive legislative authority and oversight jurisdiction over United States intelligence agencies and activities, including the mandate

> . . . to provide vigilant oversight over the intelligence activities of the United States to assure that such activities are in conformity with the Constitution and laws of the United States. (Sec. 1)

The authorities of the new Senate Intelligence Committee include surveillance and surveillance technology as practiced by the relevant

---

[3] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures. Foreign Intelligence Surveillance Act of 1976. Hearings, 94th Congress, 2d session, March 29, 30, 1976.

[4] U.S. Congress. House. Committee on the Judiciary. Subcommittee on Courts, Civil Liberties, and the Administration of Justice. Surveillance. Hearings, 94th Congress, 1st session, Feb. 6–Sept. 8, 1975.

[5] National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. Electronic surveillance. Washington, D.C.: U.S. Govt. Print. Off., 1976.

Federal agencies and its Subcommittee on the Rights of Americans has conducted hearings on the "Foreign Intelligence Surveillance Act of 1976" (S. 3197) as its initial inquiry.[6]

Prior to the creation of this Senate committee, both Chambers erected temporary select committees on intelligence to investigate allegations of illegalities, improprieties, and abuses of authority in the activities of the intelligence agencies.[7] The House Select Committee on Intelligence, created initially on Feb. 19, 1975 (H. Res. 138) and replaced by an expanded select committee possessing identical authority on July 17, 1975 (H. Res. 591), and the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (S. Res. 21, approved Jan. 27, 1975) examined aspects of surveillance technology within their domain, aspects of which are reviewed in the following survey of specific committee hearings.

The selective survey of recent congressional hearings and studies which follows is largely limited to the 93d and 94th Congresses. Consequently, the pioneering efforts of certain Congressional committees are not included. The endeavors in the 1960's by the Senate Judiciary Subcommittees on Constitutional Rights and on Administrative Practice and Procedures and of the House Government Operations Special Subcommittee on the Invasion of Privacy are prominent examples of previous congressional investigations into similar topics and issues.[8] Rep. Robert Kastenmeier, as Chairman of the House Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice, noted a lengthy heritage of congressional concern upon commencing hearings on bills relating to wiretapping and electronic surveillance:

> These hearings are not the first congressional effort to examine privacy invasion by electronic eavesdropping. Between 1934 and 1967 at least 16 sets of congressional hearings on wiretapping were held. From 1965 to 1971 former Congressman Cornelius Gallagher conducted numerous hearings on privacy invasion as chairman of the Special Subcommittee on Privacy of the House Committee on Government Operations.[9]

During this time, Congress has expressed specific concern over the use of modern technology that might potentially contribute to the erosion of personal privacy. Modern technology, coupled with increased development of Government records on individuals, has provided the background to a series of hearings prior to the 92d Congress.

---

[6] U.S. Congress. Senate. Select Committee on Intelligence. Subcommittee on Rights of Americans. Foreign Intelligence Surveillance Act of 1976. Hearings, 94th Congress, 2d session, June 30 and July 1, 1976.

[7] A review of recent and historical congressional oversight of the intelligence community is provided in a number of sources. Inter alia, Harry Howe Ransom. Congress and intelligence agencies. In Harvey C. Mansfield, Jr. (ed.). Congress against the President. Proceedings of the Academy of Political Science. v. 32, No. 1 (1975). U.S. Congress. Committee on Government Operations. Oversight of U.S. Government intelligence functions. Hearings, 94th Congress, 2d session, Jan. 21–Feb. 6, 1976. U.S. Congress. Senate. Committee on Rules and Administration. Proposed standing committee on intelligence activities. Hearings, 94th Congress, 2d session, March 31–April 5, 1976, U.S. Library of Congress. Congressional Research Service. Congressional oversight of intelligence: status and recommendations. Multilith No. 76–54 G, prepared by Frederick M. Kaiser, March 11, 1976. U.S. Library of Congress. Congressional Research Service. Congressional oversight of the intelligence community. Issue Brief No. IB76024, prepared by William Raiford, April 6, 1976. U.S. Library of Congress. Congressional Research Service. Intelligence community investigation. Issue brief No. IB75037, prepared by Richard F. Grimmett, May 28, 1975.

[8] The oversight activities of the Special Subcommittee on the Invasion of Privacy are examined by Morris Ogul. Congress oversees the bureaucracy: studies in legislative supervision. Pittsburgh: University of Pittsburgh press, 1976. 92–129.

[9] U.S. Congress, House, Committeee on the Judiciary. Subcommittee on Courtes, Civil Liberties, and the Administration of Justice. Wiretapping and electronic surveillance. Hearings, 93d Congress, 2d session, Apr. 24, 26, and 29, 1974, p. 2.

Beginning in the 1960's, both Senate and House committees held hearings on the problems of privacy and security in record handling operations.

By mid-decade the House Government Operations Special Subcommittee on Invasion of Privacy began to study the impact of technology on privacy. One of the initial set of hearings, "The Computer and Invasion of Privacy", examined some of the proposals for a National Data Bank.[10] The Chairman of the Special Subcommittee, Cornelius E. Gallagher, outlined the concern for the lack of safeguards and control over Government collecting, using, and disseminating personal information. While this set of hearings highlighted the potential dangers of a comprehensive data bank, the chairman noted that the Special Subcommittee had previously examined the problem of Federal Government personality testing and related surveys and had questioned the content of the 1964 farm census.[11]

The Senate Judiciary Subcommittee on Administrative Practice and Procedures held hearings on the concept of a Federal Data Center in 1966. In a 1967 and 1968 set of hearings the Subcommittee began an examination of Government statistics and recordkeeping efforts. Some of the problems related to computer technology and privacy were outlined in this set of hearings.[12]

In 1967 the Subcommittee also issued an inventory of Federal Government information on American citizens. This study, entitled "Government Dossier (Survey of Information Contained in Government Files)," listed the content of Government files.[13] Senator Edward V. Long, then Chairman of the Subcommittee, had sent a detailed questionnaire to all Federal agencies and requested information on the type and use of information on individuals maintained.

The Senate Judiciary Subcommittee on Constitutional Rights began hearings in 1969 on the problems associated with the Government's request for personal information.[14] These hearings in the 91st Congress considered a bill (S. 1791) "to further secure personal privacy and to protect the constitutional right of individuals to ignore unwarranted governmental requests for personal information."

The following survey of congressional hearings and documents is precluded from being a comprehensive review of activity in this area in even the most recent Congresses. Neither executive session hearings can be accounted nor can all forms or dimensions of oversight. This survey, therefore, reflects some of the major activity of the Congress and represents the variety of isues and topics examined. The selected hearings and documents are arranged into three broad categories—Senate, House of Representatives, and Joint Committee.

---

[10] U.S. Congress. House. Committee on Government Operations. Special Subcommittee on Invasion of Privacy. The computer and invasion of privacy. Hearings, 89th Congress, 2d session, July 26–28, 1966, p. 1.

[11] Ibid., p. 1.

[12] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure. Computer privacy. Hearings, 90th Congress, 2d session [Part 1], March 14–15, 1967; [Part 2], Feb. 6, 1968.

[13] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure. Government dossier. [Committee Print], 90th Congress, 1st session, 1967.

[14] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Privacy, the Census and Federal questionnaires. Hearings, 91st Congress, 1st session, April 24, 25, May 2, and July 1, 1969.

Within each category the hearings and documents are ordered by committee and subcommittee.

1. Selected Senate Hearings and Documents

"Role of the Internal Revenue Service in Law Enforcement Activities"

Holding hearings in both sessions of the 94th Congress, the Subcommittee on Administration of the Internal Revenue Code of the Senate Committee on Finance examined the "Role of the Internal Revenue Service in Law Enforcement Activities." [15] Senator Floyd K. Haskell, Chairman of the Subcommittee, and Senator Robert Dole, ranking minority member, jointly announced the purposes of the hearings, among them being the absence of court authorization for certain IRS searches and seizures, IRS access to taxpayer and third party records, and, as stated by Senator Haskell, "whether limits should be set for these (law enforcement) activities." [16] The operations and activities of the Intelligence Division of IRS were part of the institutional focus of the hearings, the objectives of which were described by Senators Haskell and Dole:

> The objective of this hearing will be to publicly air the numerous views concerning the appropriate role of the Internal Revenue Service in general Federal law enforcement efforts. One of the key issues on which these hearings will focus is the extent to which the special authority granted to the Internal Revenue Service for tax collection purposes, such as the right to conduct non-court-ordered searches and seizures and the right to administratively summon taxpayer and third party records, should also be utilized in peripheral or nontax-related Federal criminal inquiries. The discussions of this and other related issues will begin with statements by the Commissioner of Internal Revenue, Donald C. Alexander, and the Attorney General of the United States, Edward H. Levi, followed by an IRS–Justice Department panel of experts which will spell out and discuss present relationships and responsibilities.[17]

"Problems Associated with Computer Technology in Federal Programs and Private Industry—Computer Abuse"

Reflecting the growing concern with the proper use of Federal computers and the danger in improperly managed systems, the Senate Committee on Government Operations began an investigation into some of the problems related to computer security and computer abuse.[18] As part of its initial investigation and as an essential framework towards understanding the issues, the Committee included three recent reports prepared by the General Accounting Office:

"Improvements Needed in Managing Automated Decision-making by Computers Throughout the Federal Government," April 23, 1976;
"Computer-related Crimes in Federal Programs," April 27, 1976;
"Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities," May 10, 1976.

---

[15] U.S. Congress, Senate, Committee on Finance, Subcommittee on Administration of the Internal Revenue Code, Role of the International Revenue Service in law enforcement activities, Hearings, 94th Congress, 1st and 2d sesions, Dec. 1 and 3, 1975 and Jan. 22, 1976.
[16] Ibid., p. 2.
[17] Ibid., p. 1.
[18] U.S. Congress, Senate Committee on Government Operations. Problems asscociated with computer technology in Federal porgrams and private industry—computer abuse, 94th Congress, 2d session, June 1976 (At head of title—committee print).

In addition, a compilation of papers and monographs on risk assessment, privacy and security of computer systems, computer crime, and related issues was featured.[19]

In preparation for hearings the Committee began an examination of computer security with minimum emphasis on privacy problems. It was recognized that problems related to proper handling of automated information and the development of appropriate security measures have a relevant role in the future utilization of computer technology. The intent of the Committee Print is to focus on the significant management and administrative controls that would ensure proper use of computers and related technology.

"PRIVACY—THE COLLECTION, USE, AND COMPUTERIZATION OF PERSONAL DATA"

The Senate Ad Hoc Subcommittee on Privacy and Information Systems of the Committee on Government Operations and the Judiciary Subcommittee on Constitutional Rights held joint hearings on a series of bills that eventually led to the enactment of the Privacy Act of 1974.[20] These hearings held in 1974 allowed the Senate Government Operations and Judiciary Committees to continue oversight of computer usage in the Federal Government.

The primary purpose of the hearings was to determine the possible types of information containing personal identifiable data and to assess the effect of legislation on this area. Chairing the hearings, Senator Sam Ervin commented that many of the data banks previously surveyed by the Senate Subcommittee on Constitutional Rights often contained sensitive information on individuals. These files and systems rarely had specific legislative authorization. The Chairman, in reviewing the findings of the survey and introducing the new set of hearings, observed—

> I am particularly disturbed by the fact that, by and large, these data banks lack express congressional authorization. Only about one-sixth of the reported data banks could cite a specific statute which explicitly authorized the system. If congressional oversight and control are to be effective, it is essential that the other 84 percent of the reported data systems which lack express statutory authority, as well as the data banks created in the future, be required to obtain express congressional authorization. A legislative requirement that every Federal data bank be authorized by an explicit congressional mandate will also set up standards by which the Congress and private individuals can evaluate and police the operation of these systems.
>
> Requiring express statutory authorization will serve an additional purpose of giving some degree of notice to the millions of Americans about whom records are kept in data banks of which these individuals are totally unaware. The subcommittee survey shows that over 42 percent of the data banks for which responses are available give no notice of any kind to record subjects. The survey shows that the nightmare of secret data banks surreptitiously recording data about innocent Americans is, in all too many instances, a reality.[21]

---

[19] The committee print includes a brief overview of computer and information security in the Federal Government, prepared by Louise G. Becker, ibid., pp. 153–181. A copy of this memorandum is included in this report—III. B. Congressional Research Service reports.

[20] U.S. Congress. Senate. Committee on Government Operations. Ad Hoc Subcommittee on Privacy and Information Systems. Committee on the Judiciary. Subcommittee on Constitutional Rights. Privacy: the collection, use, and computerization of personal data. Joint hearings, 93d Congress, 2d session, June 18–20, 1974.

[21] Ibid., p. 4.

"WARRANTLESS WIRETAPPING AND ELECTRONIC SURVEILLANCE—1974"

In the spring of 1974, the Senate Judiciary Subcommittee on Administrative Practice and Procedure and the Subcommittee on Constitutional Rights held joint hearings on surveillance activities of selected Federal agencies.[22] In the opening statement, Senator Edward M. Kennedy, Chairman of the Subcommittee on Administrative Practice and Procedure, noted that the joint hearings would examine the basis for employing electronic surveillance by the Federal Government. Senator Kennedy outlined the main focus of the hearings in the following statement:

> During these hearings we will be trying to determine exactly what definition of "national security" has been used as a basis for warrantless electronic surveillance in the past, and what definition should be used in the future.
>
> We will want to know whether the information gathered from these surveillances justifies the intrusion they impose and the potentials for abuse they entail.
>
> We will be asking about the historical background of warrantless wiretapping, and Executive's current interpretation of legal restrictions placed on it.
>
> We will be examining the justifications and procedures involved in the tapping of the 17 Government officials and newsmen, plus others which have recently come to light.
>
> We will be inquiring as to how many agencies conduct warrantless surveillances, and under what guidelines.[23]

"CRIMINAL JUSTICE DATA BANKS—1974"

In the 93rd Congress, the Senate Judiciary Subcommittee on Constitutional Rights held hearings on the control and regulation of criminal justice information systems.[24] The Subcommittee considered four bills designed to improve the regulations—S. 2542, S. 2810, S. 2963, and S. 2964. Senator Sam J. Ervin, Jr., then chairman of the Subcommittee, in his opening statement outlined some of the major concerns in the development of criminal justice information legislation. The following problems were identified as requiring additional consideration:

Incomplete records—the need to include disposition information on all disseminated arrest records;

Challenges to the information for accuracy and completeness by the individual;

The scope and nature of possible civil remedies to enforce dissemination regulations;

The collection and dissemination of intelligence or investigatory files; and

The need to identify who is to control and operate both manual and automated criminal justice systems.[25]

---

[22] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure. Subcommittee on Constitutional Rights. Warrantless wiretapping and electronic surveillance—1974. Hearings, 93d Congress, 2d session, April 3 and 8, May 8–10 and 23, 1974.

[23] Ibid., p. 2.

[24] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Criminal Justice Data Banks—1974. Hearings. 93rd Congress, 2nd Sess. March 5–7, 12–14, 1974.

[25] Ibid., pp.6–7.

"CRIMINAL JUSTICE INFORMATION AND PROTECTION OF PRIVACY ACT OF 1975"

In the 94th Congress the Senate Judiciary Subcommittee on Constitutional Rights conducted hearings on the control and regulation of criminal justice information to ensure the protection of individual privacy.[26] The hearings focused on three legislative proposals, S. 2008, S. 1427, and S. 1228, which call for the regulation of criminal justice information.

Senator John V. Tunney, Chairman of the Subcommittee, in his opening remarks, commented on the dangers inherent in the improper use of criminal justice information.[27] The Chairman expressed specific concerns over the increased computerization of criminal justice information systems and the need to place appropriate restraints over the use and dissemination of this information.

Witnesses at the hearings emphasized the need to improve present protective mechanisms while establishing additional guides and standards to allow States and local governments to continue their essential role in the collection, use, and dissemination of criminal justice information. The vital role of State and local government in the development and implementation of these information systems, according to testimony, could be augmented with appropriate examination and subsequent recommendations.

"FEDERAL DATA BANKS, COMPUTERS, AND THE BILL OF RIGHTS"

In 1971 the Senate Judiciary Subcommittee on Constitutional Rights, chaired by Senator Sam Ervin, began hearings on the collection of personal information by the Federal Government.[28] The chairman voiced the concern that the protection of personal privacy was becoming more difficult in face of the "information power of government." [29] Senator Ervin observed that Americans had expressed a concern for the growing Federal propensity to collect and disseminate personal information. He described the catalyst of the hearings in the following words:

> These hearings were called because it is clear from the complaints being received by Congress that Americans in every walk of life are concerned about the growth of government and private records on individuals. They are concerned about the growing collection of information about them which is none of the business of the collectors.
>
> They are concerned about the confidentiality and security of the information on them which is in the hands of those whose decisions can affect their lives for better or worse.
>
> They are concerned that they are constantly being intimidated, coerced, or pressured into revealing information to the wrong people, for the wrong purpose, at the wrong time.
>
> They are concerned that this information is being automated or computerized without proper screening or controls.

---

[26] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Criminal justice information and protection of Privacy Act of 1975. Hearings. 94th Congress, 1st session, 1975.

[27] Ibid., pp. 1–2.

[28] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Federal Data Banks, Computers and the Bill of Rights. Hearings. 92d Congress, 1st Sess., Feb. 23, 24, and 25, March 2–4, 9–11, 15, 17, 1971.

[29] Ibid., p. 1.

But, above all, they are worried that the existing laws are no longer sufficient to protect the privacy of the individual against the "information power" of government.[30]

One of the computerized information-gathering programs highlighted in the hearings was the Army intelligence computer at Fort Holabird. This information base contained surveillance data on civilians active in politics and related matters. The file was to provide information on possible civil disturbances "or prevent service men from being subjected to influences which would lower morale." [31]

"FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS"

As part of an extensive examination of Federal Government data banks, the Senate Subcommittee on Constitutional Rights issued a survey on personal identifiable information systems.[32] The six volume committee print is Part III of the Subcommittee's continuing study and hearings entitled "Federal Data Banks, Computers, and the Bill of Rights." This study examines some of the information on individual rights and highlights the extent of Federal holdings of personal data. The intent of the study was to determine the scope and nature of Federal data banks. The Subcommittee noted that this survey indicated a need for a statutory requirement to provide a comprehensive reporting of Government holding and, in commenting on the survey, observed that—

Now that the survey has been completed, these preliminary observations have been substantiated. The most significant finding is that there are immense numbers of government data banks, littered with diverse information on just about every citizen in the country. The 54 agencies surveyed were willing to report 858 of them, containing more than 1¼ billion records on individuals.

Finding out about these systems has been a difficult, time-consuming, and frustrating experience. The inherent aversion of the Executive Branch to informing Congress and the people about what they are doing is not restricted to matters of high-policy, national security, or foreign policy. An attitude approaching disdain infects even requests for basic non-sensitive data such as this survey sought. The subcommittee met evasion, delay, inadequate and cavalier responses, and all too often a laziness born of a resentment that anyone should be inquiring about their activities. Some agencies displayed their arrogance by not replying at all. With others, extracting information was like pulling teeth. These remarks should not detract from our appreciation for the fine cooperation the subcommittee received from a great many agencies.

The most basic lesson the subcommittee's survey teaches is the absolute necessity of replacing this voluntary survey approach with a statutory requirement that all federal data banks be fully and accurately reported to the Congress and the American people. This study of Federal Data Banks and Constitutional Rights also demonstrates the need for requiring:

explicit statutory authority for the creation of each data bank, as well as prior examination and legislative approval of all decisions to computerize files;

privacy safeguards built into the increasingly computerized government files as they are developed, rather than merely attempting to supplement existing systems with privacy protections;

notification of subjects that personal information about them is stored in a Federal data bank and provision of realistic opportunities for individual subjects to review and correct their own records;

[30] Ibid., p. 1.
[31] Ibid., p. 5.
[32] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Federal Data banks and constitutional rights. A study of data systems on individuals maintained by agencies of the United States Government. Volumes 1–6. 93d Congress, 2d session, 1974. [At head of title: committee print]

constraints on interagency exchange of personal data about individuals and the creation of interagency data bank cooperatives;

the implementation of strict security precautions to protect the data banks and the information they contain from unauthorized or illegal access;

continued legislative control over the purposes, contents and uses of government data systems.[33]

"MILITARY SURVEILLANCE"

The Senate Committee on the Judiciary's Subcommittee on Constitutional Rights held hearings in April, 1974, on S. 2318, a bill to prohibit the military from conducting surveillance of civilian political activities or organizations.[34] While limiting military surveillance, the bill specifies certain exceptions. The subcommittee's previous reports, "Army Surveillance of Civilians: A Documentary Analysis" (1972) and another entitled "Military Surveillance of Civilian Politics" (1973), outlined the extent of surveillance by the Department of Defense (DOD) and the DOD Directive which places restrictions on surveillance of civilians. In the hearings, the Constitutional Rights Subcommittee recognized the creation of the Defense Investigative Review Council (DIRC) as a positive step in providing essential safeguards and regulating surveillance activities in keeping with the DOD mission. The subcommittee noted that DOD had made some progress in limiting and controlling inappropriate surveillance activities but that it was not entirely satisfied with the range of activities remaining.

Senator Sam Ervin, then Chairman of the Subcommittee on Constitutional Rights, concluded that there was a need to provide protection to the individual from overzealous military surveillance. The subcommittee hearings focused on the extent that DOD had fully implemented the Defense Directive (5200.27, March 1, 1971) "governing the collection and retention of information on the political activities of Americans unaffiliated with the Armed Services." Senator Ervin, by way of conclusion, voiced the need for remedies to such surveillance stronger than a Defense Department directive.

"POLITICAL INTELLIGENCE IN THE INTERNAL REVENUE SERVICE; THE SPECIAL SERVICE STAFF"

In 1974, the Subcommittee on Constitutional Rights of the Senate Judiciary Committee authorized a documentary analysis by its staff regarding "Political Intelligence in the Internal Revenue Service: The Special Service Staff." Released in December of 1974, the report was the second such summary of political surveillance operations in the Federal Government produced by the Subcommittee, the first being an inquiry into Army surveillance, 1970–1974. The investigation of the Special Service Staff of IRS was restricted by the lack of authority of the Constitutional Rights Subcommittee to examine tax records. Nonetheless, the extensive review elicited the following conclusion from Subcommittee Chairman Sam J. Ervin:

The purpose of the Internal Revenue Service is to enforce the tax laws, not to enforce political orthodoxy. The Special Service Staff operations represent a

[33] Ibid., pp. iv–v.

[34] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Military surveillance. Hearings, 93d Congress, 2d session, April 9, 10, 1974.

dangerous abuse of the enormous powers Americans have given to the tax collection arm of government.[35]

Generated initially by the Watergate investigations of the preceding year, the Constitutional Rights investigation of the Special Service Staff discovered that the group, which existed from 1969 to 1973, was used to seek out information on political activist organizations and the individuals on the "enemies list" compiled by the White House in the Administration of Richard Nixon. The Special Service Staff (SSS) developed its own files on individuals which contained information which did not relate to possible violations of Internal Revenue Service laws according to the Subcommittee report. The report also contained documentation regarding SSS acquisition of information on subjects from the Social Security Administration, the House Committee on Internal Security, and Army Intelligence, as well as SSS cooperation with the Internal Security Division of the Justice Department.

"PRIVACY, POLYGRAPHS, AND EMPLOYMENT"

The staff of the Senate Judiciary Subcommittee on Constitutional Rights prepared a study entitled "Privacy, Polygraphs, and Employment," released in 1974.[36] As part of a continuing series of studies on the right of privacy sponsored by the subcommittee, this endeavor complemented earlier analyses, according to Subcommittee Chairman Senator Sam J. Ervin, Jr.:

> These efforts have been aimed at curbing unwarranted governmental invasions of the privacy of individual citizens. The use of polygraph testing for employment purposes has been one such threat investigated by the Subcommittee.[37]

The staff study examined employer use of the polygraph vis-a-vis employee right of privacy, the reliability of polygraph tests, their constitutionality and current status. The study concluded that evidence clearly indicated that the polygraph test "is here to stay. And, given modern ingenuity, it is not unreasonable to expect that new techniques and devices will be devised in an attempt to facilitate determining honesty." [38] In noting recent developments in the technology, the staff asserted that "These two innovations indicate that rather than being curtailed, use of the polygraph is being expanded, particularly in private business." [39]

Given the state of this particular surveillance technology, the staff study recommended the following:

> Limits, beyond which invasions of privacy will not be tolerated, must be established. The Congress should take legislative steps to prevent Federal agencies as well as the private sector from requiring, requesting, or persuading any employee or applicant for employment to take any polygraph test. Privacy is a fundamental right that must be protected by prohibitive legislation from such unwarranted invasions.[40]

---

[35] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Political Intelligence in the Internal Revenue Service: the Special Service Staff. A Documentary Analysis prepared by the staff of the Subcommittee on Constitutional Rights. 93d Congress, 2d session, December 1974 (Committee print), p. iv.

[36] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Privacy, polygraphs and employment. (Study prepared by staff). 93d Congress, 2d session, November 1974 (At head of title: committee print).

[37] Ibid., p. 11.

[38] Ibid., p. 16.

[39] Ibid., p. 17.

[40] Ibid., p. 18.

"SURVEILLANCE TECHNOLOGY"

The joint hearings of the Senate Judiciary Subcommittee on Constitutional Rights and the Senate Commerce Special Subcommittee on Science, Technology, and Commerce explored some of the issues related to the use of surveillance technology.[41] The complexity of the problems from both the legal and technical aspects are outlined in hearings.

Senator John V. Tunney, Chairman of the Subcommittee, provided a framework for the hearings noting that the hearings would examine the following problems:

> The Government's role in researching, devleoping, using and disseminating the technological means of invading privacy and otherwise intruding upon the constitutional rights of American citizens; the adequacy of government's present structures and procedures in the area of science policy for assessing the social impacts of new technology that either is designed specifically for surveillance or has derivative surveillance applications; the investment of the taxpayer's dollar to determine whether massive spending on surveillance technology has the effect of wasting scarce public funds and distorting priorities in both the public and private sectors; and the effectiveness of the administration of our present laws, and the possible need for new legislation, to regulate the growth of surveillance technology in both the public and private sectors.[42]

Included in the hearings were transcripts of a series of news broadcasts by Ford Royan of NBC which outlined some of the possible problems associated with computer communication networks and the interrelationship with the concept of privacy and national data banks.

"FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1976"

Hearings on proposals regarding the "Foreign Intelligence Surveillance Act of 1976" were held by the Subcommittee on Criminal Laws and Procedures of the Senate Judiciary Committee during March of 1976. The bills before the subcommittee—S. 743, S. 1888, and S. 3197, the last of which is identical to a measure transmitted to the Senate by President Ford—deal with electronic surveillance for foreign intelligence and national security purposes. The hearings focused on several main issues, including the absence of explicit judicial requirements for warrants for national security electronic surveillance of individuals, the lack of statutory controls over the conduct of electronic surveillance for national security purposes, the abuses of Presidential power in the surveillance area, and the infringements on civil liberties and rights inherent in certain surveillance practices.

One of the sponsors of the bills, Senator Edward Kennedy, summarized the necessity of further legislation in this area:

> The abuses of Presidential power in the surveillance area reached their zenith under the Nixon administration. And yet, electronic surveillance can also be constructive and useful as a carefully limited, circumscribed tool for gathering certain information truly essential to our national defense. Both the importance of wiretapping, and the dangers inherent in such surveillance—governmental intrusion into the private lives and conversations of Americans and

[41] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Committee on Commerce. Special Subcommittee on Science, Technology, and Commerce. Surveillance technology. Hearings. 94th Congress, 1st session, June 28 and Sept. 9, 10, 1975.

[42] Ibid., p. 2.

interference with the Constitutionally protected rights of privacy, association and speech—dictate that Congress take quick, effective action.

By expressly incorporating into law the requirement of a judicially approved warrant procedure, by explicitly mandating that both the President and his designate certify in writing the need for such surveillance, and, perhaps, most importantly, by limiting the scope of such surveillance, to those persons acting "pursuant to the direction of a foreign power," this legislation seeks to substitute carefully prescribed accountability and oversight for the arbitrariness of the past.[43]

On June 15, 1976, the Senate Judiciary Committee voted eleven to one to report out favorably S. 3197, actually a Subcommittee amendment in the nature of a substitute to the original version.[44] The lone objector, Senator John Tunney, listed nineteen weaknesses with the legislation as drafted, which "gives official sanction to surveillance procedures which are ripe for misuse." [45] Senator Tunney continued—

S. 3197 treads on dangerous ground, enlarging the Government's authority for bugging, wiretaps, unspecified "other" surveillance devices, and break-ins to install them . . . The enumerated justifications for surveillance are so broad that a future administration may easily misuse its powers for political purposes. The power to tap can be the power to destroy. The bill gives the illution, but not the reality, of curtailing the surveillance abuses revealed by the Church committee, and so may postpone real reform in this area. It may be read as a congressional seal of approval for those abuses. If the available choices before Congress were restricted to S. 3197 or no bill, it would be preferable to defeat this bill and wait for the next administration's proposals.[46]

"ELECTRONIC SURVEILLANCE FOR NATIONAL SECURITY PURPOSES"

Responding to several legislative proposals in the 93d Congress, the Senate Judiciary Subcommittees on Criminal Laws and Procedures and on Constitutional Rights held joint hearings on "Electronic Surveillance for National Security Purposes." [47] These bills (S. 2820, S. 3440, and S. 4062) and subsequent hearings were precursors to their counterparts in the 94th Congress dealing with the "Foreign Intelligence Surveillance Act of 1976." Senator John McClellan, Chairman of the Criminal Laws and Procedures Subcommittee, recognized the unprecedented nature of the 1974 hearings in his opening statement:

S. 2820—the subject of the hearings this morning, would for the first time in this country's history attempt to place stringent restrictions on the President's power to use electronic surveillance against foreign powers and foreign nationals for national security intelligence purposes. It would require the President to seek a judicial warrant and to carry the burden of establishing probable cause that such character of surveillance is necessary (1) to protect the Nation against actual or potential attack or other hostile acts of a foreign power, or (2) to obtain foreign intelligence information deemed essential to the security of the United States, or (3) to protect national security information against foreign intelligence activities. The probable cause showing must be on evidence, independent of the President's or of others' conclusory opinion that the surveillance is necessary for these purposes.

---

[43] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures. Foreign Intelligence Surveillance Act of 1976. Hearings. 94th Congress, 2d session, March 29, 30, 1976, p. 3.

[44] U.S. Congress. Senate. Committee on the Judiciary. Foreign Intelligence Surveillance Act of 1976. Report together with additional and minority views (to accompany S. 3197). 94th Congress, 2d session, July 15, 1976, p. 7.

[45] Ibid., p. 129.

[46] Ibid., p. 123.

[47] U.S. Congress. Senate. Committee on the Judiciary. Subcommittees on Criminal Laws and Procedures and on Constitutional Rights. Electronic surveillance for national security purposes. Joint hearings (on S. 2820, S. 3440, and S. 4062). 93d Congress, 2d session, Oct. 1, 2, and 3, 1974.

The bill makes no provision for national security intelligence surveillance of United States citizens acting as foreign agents—a question carefully left open by the Supreme Court in *United States* v. *United States District Court*, 407 U.S. 297, 309 Note 8 (1972). It prohibits issuance of a warrant even as to foreign nationals unless the President can show that the alien's first allegiance is to a foreign power, that he is working to serve the interest of that foreign power and that he is working to undermine the security of the United States. Also, evidence obtained under a valid warrant cannot be used in a criminal trial. As the hearings progress, other restrictions on the President's power will no doubt be developed.[48]

"FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1976"

The Subcommittee on the Rights of Americans of the newly-formed Senate Select Committee on Intelligence conducted its initial hearings into the "Foreign Intelligence Surveillance Act of 1976" (S. 3197).[49] Closed and open hearings had been held in June and July, 1976, and testimony received from representatives of Government departments and agencies which utilized information secured through electronic surveillance, including Attorney General Edward H. Levi.

The proposed legislation attempts to establish statutory guidelines regarding wiretapping and electronic surveillance for national security purposes, which presently are exempted from such guidelines, The "Foreign Intelligence Surveillance Act of 1976" recognized the current absence of court-approved warrants for national security electronic surveillance and proposed a judicially approved warrant procedure, incorporating the requirement that the President or his designate certify in writing the need for such surveillance.

"PRESIDENTIAL CAMPAIGN ACTIVITIES"

The Senate Select Committee on Presidential Campaign Activities, commonly referred as the "Watergate Committee," conducted extensive hearings into abuses and illegal actions associated with the 1972 Presidential campaign. Held during the summer of 1974, the hearings elicited evidence of widespread illegal activity associated with the break-in of the Democratic National Committee headquarters at the Watergate complex and the subsequent attempted cover-up of the investigation.

The abuse of intelligence and surveillance authority and the political manipulation of law enforcement/intelligence agencies by the White House was summarized by the Chairman of the Select Committee, Senator Sam J. Ervin, Jr., in the closing remarks of the Committee's final report:

> They had forgotten, if they ever knew, that the Constitution is designed to be a law for rulers and people alike at all times and under all circumstances; and that no doctrine involving more pernicious consequences to the commonweal has ever been invented by the wit of man than the notion that any of its provisions can be suspended by the President for any reason whatsoever.
>
> On the contrary, they apparently believed that the President is above the Constitution, and has the autocratic power to suspend its provisions if he decides in

---

[48] Ibid., p. 3.

[49] U.S. Congress. Senate. Select Committee on Intelligence. Subcommittee on the Rights of Americans. Hearings. 94th Congress, 2d session, June 29 and 30 and July 1, 1976. The Senate Select Committee issued a report favoring an amended version of S. 3197 by a vote of 14 to 1. U.S. Congress. Senate. Select Committee on Intelligence. Foreign Intelligence Surveillance Act of 1976. Report together with additional views (to accompany S. 3197). 94th Congress, 2d session, August 24, 1976. Senate Report 94–1161.

his own unreviewable judgment that his action in so doing promotes his own political interests or the welfare of the Nation. As one of them testified before the Senate Select Committee, they believed that the President has the autocratic power to suspend the fourth amendment whenever he imagines that some indefinable aspect of national security is involved. [50]

According to the Select Committee inquiries, the Constitutional protections for basic civil liberties were infringed on by certain manipulations of the surveillance powers of the executive branch. Among these were the creation of a White House special investigations unit, known as the "Plumbers," which conducted illegal and surreptitious surveillance, following the aborted establishment of an inter-departmental intelligence unit as outlined in the "Huston plan;" the development of an "enemies list" in 1971, prepared by Presidential Counsel John Dean, for special investigation by the Internal Revenue Service and to make the intelligence capabilities of "I.R.S. politically responsive;" White House-inspired electronic surveillance; creation of an offensive intelligence-gathering capability within the White House; requests for taxpayer information from the IRS; misuse and attempted misuse of intelligence information of the FBI, Department of Justice, Secret Service and other agencies; and an attempt to utilize the Central Intelligence Agency to retard the FBI inquiry into the Watergate break-in. [51]

"GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES"

Following public revelations about alleged illegal and unethical conduct on the part of the Central Intelligence Agency, the Senate created the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Meeting from February 1975, until release of its final report in April of 1976, the select committee held hearings on a number of intelligence agencies in addition to the CIA and examined a variety of intelligence and surveillance practices.

Regarding the structure, history, activities and policies of America's most important intelligence agencies, the Committee addressed three broad questions:

First, whether domestic intelligence activities have been consistent with law and with the individual liberties guaranteed to American citizens by the Constitution.

Second, whether America's foreign intelligence activities have served the national interest in a manner consistent with the nation's ideals and with national purposes.

Third, whether the institutional procedures for directing and controlling intelligence agencies have adequately ensured their compliance with policy and law, and whether those procedures have been based upon the system of checks and balances among the branches of government required by our Constitution.[52]

The extensive hearings focused on a number of prominent issues relating to electronic surveillance, the controls over such operations, and their policy implications. The select committee examined the use of improper or illegal means for gathering domestic intelligence, includ-

[50] U.S. Congress. Senate. Select Committee on Presidential Campaign Activities. Final Report. 93d Congress, 2d session, June 1974. Senate Report No. 93–981, p. 1102.
[51] Ibid., passim.
[52] U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Intelligence Activities and the Rights of Americans (Book II). Final Report. 94th Congress, 2d session, April 26, 1976. Senate Report No. 94–755, pp. vi–vii.

ing indiscriminate mail openings by the CIA and the FBI, National Security Agency receipt of international cables sent by American citizens, frequent wiretapping and bugging of American citizens without judicial warrant since the 1930's by intelligence agencies, the absence of prior approval by the Attorney General for warrantless wiretaps despite its requirement, the unregulated nature of micophone suveillance by intelligence agencies for certain classes of cases, the collection and dissemination of purely political and personal information through electronic surveillance conducted by intelligence agencies, innumerable warrantless break-ins by certain intelligence agencies in order to install microphones for surveillance purposes, and the obtaining of confidential tax return information by the FBI as part of the Bureau's counter-intelligence program.[53]

These illegal or improper operations and practices, according to the Select Committee's final report, had several adverse impacts—discrediting of citizens, manipulation of the media, distortion of data to influence Government policy and public perceptions, "chilling" effect on First Amendment rights of citizens, preventing the free exchange of ideas, and extremely high costs for operations which proved on occasion to be counterproductive or of limited value.

The Senate select committee on intelligence recommended a series of reforms to control abuses and excesses relating to intelligence practices and surveillance. In sum, the select committee concluded that "Clear legal standards and effective oversight and controls are necessary to ensure that domestic intelligence activity does not itself undermine the democratic society it is intended to protect." [54]

2. Selected House Hearings and Documents

"Oversight Hearings into the Operations of the IRS"

"Oversight Hearings into the Operations of the IRS" were conducted by the House Government Operations Subcommittee on Commerce, Consumer, and Monetary Affairs during the 1st session of the 94th Congress. The broad concern was with the interrelationship of IRS with other Federal agencies, the operations of the IRS, and Treasury Department-IRS policies and practices regarding intelligence collection and utilization. The subcommittee chariman, Rep. Benjamin Rosenthal, introduced the hearings by emphasizing the following issues:

> We have seen evidence with the disclosure of the enemies list, of attempts to politicize and misuse the IRS. There have recently been allegations of corruption, unauthorized bugging, and wiretapping, and abuse of power involving the Service. Some believe that in the audit, inspection and collection areas, IRS resources have been weighted too heavily against small individual taxpayers as opposed to corporate taxpayers. Others claim that IRS has lost its proper direction. These individuals maintain that IRS has gone from being the Nation's principal collector of taxes to its principal enforcer of Federal criminal laws. In this regard there is a dispute as to who supervises and controls the activities of IRS intelligence agents in the pursuit of certain law enforcement objectives and whether

[53] Ibid., pp. 10–13.
[54] Ibid., p. 20.

such objectives fall within the proper scope of the Service's mission to collect taxes and enforce tax laws.[55]

The subcommittee proceeded to examine the instances of unauthorized electronic surveillance by IRS, the inventory of mechanical and/or electronic devices in custody of the Intelligence Division and the Inspection Service's Internal Security Division, "Operation Leprechaun," and other IRS intelligence operations.

"ACCESS TO RECORDS"

The House Committee on Government Operations Subcommittee on Foreign Operations and Government Information held hearings in the 93rd Congress on the legislation that would provide the framework for the Privacy Act of 1974.[56] The Chairman of the Subcommittee, Rep. William S. Moorhead, commented on the legislation under consideration:

> This legislation would permit all Americans to know, in most cases, what files their Government maintains on them, the contents of such files, and how they are used by Federal agencies. It would grant inspection, correction, transfer notification, and other basic protection rights.
>
> The importance of such legislation has been brought vividly to the attention of the public by the abuses uncovered in the Senate Watergate investigation and by this country's great free press. One publication said only a few weeks ago the real tragedy of Watergate is that for the first time many Americans are beginning to fear their own Government.[57]

The Chairman went on to observe the Congress has the responsibility to enact laws that implement the spirit of the Constitution and that both the Freedom of Information Act and the privacy legislation under consideration would contribute towards this end.

"RECORDS MAINTAINED BY GOVERNMENT AGENCIES"

In the 92d Congress, the House Government Operations Subcommittee on Foreign Operations and Government Information held hearings on proposals (H.R. 9527) and related bills) providing that individuals be apprised of records concerning them maintained by Government agencies.[58] The hearings were designed to examine the various and extensive records systems maintained by the Federal Government on private citizens and Federal employees. Subcommittee Chairman William S. Moorhead introduced the first session by emphasizing the concern with the potential misuses of such systems:

> Some argue that we have already reached, 12 years early, the "Big Brother" era made famous in Orwell's novel, "1984." There is much evidence that they may be right. Massive computer data banks hold records of every conceivable kind on millions and millions of Americans and such records are used for hundreds of purposes, from credit reporting checks, income tax returns, the issuance of driv-

---

[55] U.S. Congress. House. Committee on Government Operations. Subcommittee on Commerce, Consumer, and Monetary Affairs. Oversight Hearings into the Operations of the IRS. Hearings, 94th Congress, 1st session, May 14–July 31, 1975. pp. 1–2.

[56] U.S. Congress Congress. House. Committee on Government Operations. Subcommittee on Foreign Operations and Government Information. Access to records. Hearings, 93rd Congress, 2d session, Feb. 19, 20; April 30; May 16, 1974.

[57] Ibid., p. 1.

[58] U.S. Congress. House. Committee on Government Operations. Subcommittee on Foreign Operations and Government Information. Records maintained by Government agencies. Hearings, 92d Congress, 2d session, June 22 and 27, 1972.

ers' licenses, the maintenance of personnel information, security investigation files, social security records, and many other similar types of information.[59]

One of the sponsors of the relevant legislation, Rep. Edward I. Koch, noted Congress' propitious rejection of a National Data Center several years previous, the existence of nearly 6,000 computers in use by the Federal Government at that time, the innumerable files maintained throughout the agencies, and the absence of legislative regulations governing Government computer usage.[60] In consequence, he emphasized the need for privacy safeguards to be established, some of which were eventually incorporated in the Privacy Act of 1974.

The Director of the Bureau of Personnel Investigations of the Civil Service Commission (CSC), which houses the largest number of individual files, testified with respect to CSC procedures and standards in personnel investigations. The Director emphasized that certain surveillance techniques were prohibited to investigators, including polygraph and lie detectors, phone or wiretaps, listening devices, mail covers, searches and seizures on private property, paid informants, and visual surveillance.[61]

"IMPLEMENTATION OF THE PRIVACY ACT OF 1974: DATA BANKS"

The House Government Operations Subcommittee on Government Information and Individual Rights (formely the Subcommittee on Foreign Operations and Government Information) held hearings on the Federal Government efforts to implement the Privacy Act of 1974.[62] The hearings heard testimony from the Office of Management and Budget on the issuance of guidelines and standards as directed by the Act. In addition, the Department of Defense, Justice, and Health, Education and Welfare outlined their efforts in preparing for the full implementation of the Privacy Act.

"INTERCEPTION OF NONVERBAL COMMUNICATIONS BY FEDERAL INTELLIGENCE AGENCIES"

During the first and second sessions of the 94th Congress, the House Government Operations Subcommittee on Government Information and Individual Rights held a series of hearings on the interception of nonverbal communications by Federal intelligence agencies.[62a] The agencies examined included the Federal Bureau of Investigation, the National Security Agency, and the Civil Division of the Department of Justice. The purposes of the hearings were stated by Subcommittee Chairperson Bella Abzug:

> (W)e are considering allegations that the FBI, the National Security Agency, and perhaps other Federal agencies or their agents have for many years intercepted some or all of the wire and radio traffic being transmitted to or from this country by various communications companies. We are also interested in

[59] Ibid., p. 8.
[60] Ibid., pp. 39–40.
[61] Ibid., p. 68.
[62] U.S. Congress. House. Committee on Government Operations. Subcommittee on Government Information and Individual Rights. Implementation of the Privacy Act of 1974: data banks. Hearings, 94th Congress, 1st session, June 3, 1975.
[62a] U.S. Congress. House. Committee on Government Operations. Subcommittee on Government Information and Individual Rights. Interception of nonverbal communications by Federal agencies. Hearings, 94th Congress, 1st and 2d session, October 23, 1975 . . . March 11, 1976.

the interception of communications which were both sent and received in the United States.[62b]

During the investigation, the Subcommittee examined some of the relationships between Federal authorities and private companies, such as International Telephone and Telegraph World Communications, Inc., RCA Global Communications, and Western Union International, which assist the surveillance operations. It was during the investigations that "Operation Shramrock" by the NSA was acknowledged, revealing that three major international communications carriers turned over copies of their international cables to NSA. The Agency then selected "about 150,000 messages a month" for analysis and review.[62c]

Subcommittee attempts to acquire data and information from the private corporations and NSA resulted in assertions of executive privilege by President Ford to withhold them.

"FCC MONITORING OF EMPLOYEES' TELEPHONES"

Expressing concern for the privacy rights of Federal employees, the Special Subcommittee on Investigations of the House Committee on Interstate and Foreign Commerce reviewed "FCC Monitoring of Employees' Telephones." These hearings, held on March 28 and May 16, 1972, examined allegations of an earlier practice at the Federal Communications Commission. The subcommittee chairman emphasized oversight responsibilities with regard to the following revelation:

> Our information is that in February 1970, a secret extension phone was run from a telephone on the third floor of the FCC headquarters to the office of the agency's security officer on the eight floor. Its purpose was allegedly to surreptitiously monitor telephone conversations carried on the third floor telephone. Our information is also that this surreptitious surveillance was actually carried out over a period of 5 weeks.[63]

The irony that the FCC had conducted secret surveillance was noted by the subcommittee chairman as was the seriousness of the operation:

> The FCC, more than any other agency, ought to be especially sensitive about wiretapping because that is where the law forbidding wiretapping began. The provision against wiretapping was originally part of the Communications Act. In circumstances not involving national security, the law specifically forbids any eavesdropping unless at least one of the parties whose telephone calls are intercepted has consented to the tap, or unless a court order has been obtained. In the present case, it appears that there was neither consent nor a court order.[64]

"DISSEMINATION OF CRIMINAL JUSTICE INFORMATION"

In both sessions of the 93rd Congress, the House Subcommittee on Civil Rights and Constitutional Rights (formerly Subcommittee no. 4) of the Judiciary Committee continued hearings on the regulation of criminal justice information.[65] While these hearings focused on the

---

[62b] Ibid., pp. 157–158.
[62c] Ibid., p. 158.
[63] U.S. Congress. House. Committee on Interstate and Foreign Commerce. Special Subcommittee on Investigations. FCC Monitoring of Employees' Telephones. Hearings. 92d Congress, 2d session, March 28 and May 16, 1972, p. 1.
[64] Ibid., pp. 9–10.
[65] U.S. Congress. House. Committee on the Judiciary. Subcommittee on Civil Rights and Constitutional Rights. Dissemination of criminal justice information. Hearings, 93d Congress, 1st and 2d sessisons, July 26, 1973–April 3, 1974.

problems of limiting the distribution of arrest records, they also highlighted those associated with effective administration of regulations on criminal justice information systems.

Under consideration by the Subcommittee were the following bills: H.R. 188 (previously introduced in the 92d Congress as H.R. 13315), which concentrated on the regulation of arrest records; H.R. 9783, which provided for regulation of the collection, storage, and dissemination of information by criminal justice data banks established or supported by the Federal Government; and H.R. 12574 and H.R. 12575, which outlined more specifically the limitations and controls of criminal justice information.

At the opening of the 1974 hearings, the House Judiciary Chairman, Representative Peter W. Rodino, Jr., commented on some of the difficult problems that must be addressed. Chairman Rodino observed:

> Everyone recognizes, and I support the theme, that law enforcement agencies need efficient and effective information to aid them in pursuit of their duties. The mobility and complexities of interstate crime and criminals also demands a national crime information center. But it seems to me that the rapid expansion of our capabilities, knowledge in the area of electronics, computers, and our worship of the gathering of statistics and information is presently out of balance with our concern for the individual's right of privacy. Our technology has outdistanced our ability to preserve these basic rights and is in danger of permanently outstripping it if we do not restore and provide for the maintenance of that delicate balance.[66]

Other witnesses acknowledge the need to protect individuals from potential misuse of the systems. They cautioned that the complexity of the criminal justice systems did not allow for either a quick or easy solution to the basic dilemma—the needs of the criminal justice agencies and the problems of privacy must be brought into an appropriate balance.

"SURVEILLANCE"

In 1975 the House Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice began extensive hearings on wiretapping and electronic surveillance.[67] Representative Robert W. Kastenmeier, Chairman of the Subcommittee, in his opening address, remarked that there was a need to examine Government wiretapping and surveillance activities and operations in light of recent revelations. He observed that both public and private sectors were concerned with the extent of Government intervention in the lives of citizens and listed "wiretapping, the use of surreptitious entry and the bugging of homes" as being some of the activities that required increased oversight. Since the threat of warrantless wiretapping was considered most difficult to deal with, the chairman emphasized that the potential misuse of the technology "could form the cornerstone of a future police state." [68]

Representative Kastenmeier called attention to the numerous legislative proposals that have been introduced in the 94th Congress and noted—

---

[66] Ibid., pp. 211–212.
[67] U.S. Congress. House. Committee on the Judiciary. Subcommittee on Courts, Civil Liberties, and the Administration of Justice. Surveillance. Hearings, 94th Congress, 1st session, Feb. 6–Sept. 8, 1975.
[68] Ibid., p. 2.

The various bills presently pending before the subcommittee outline the broad scope of the problem and suggest a number of possible solutions. They range from proposals to ban any investigation of American citizens for other than limited criminal law enforcement or job application purposes to a bill which bans all military surveillance of civilians. Other legislation would require court orders for one-party consensual wiretapping or for national security electronic eavesdropping. The specific proposal which today's witnesses will address would prohibit intelligence gathering and surveillance by wiretapping, mail opening, inspection of bank, telephone, credit, and other personal records without a court order based on probable cause that criminal activity is involved.[69]

In addition to the legislative proposals, the hearings examined possible litigation which might result from abuses in Government surveillance.

"WIRETAPPING AND ELECTRONIC SURVEILLANCE"

The House Committee on the Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice held hearings in the 94th Congress on matters relating to wiretapping and electronic surveillance.[70] Representative Robert W. Kastenmeier, Chairman of the Subcommittee, related the main concern—that without proper controls and regulation on technology, individual privacy might be eroded. He proceeded to outline some of the problems:

Within the last several years many citizens have begun to fear that this basic right is being steadily eroded by the use of modern technology to eavesdrop on conversations. Unfortunately, increasing numbers of Americans have begun to fear that Government is more interested in intruding into their private lives than in acting to protect their privacy. A basic purpose of these hearings is to examine the trend toward privacy invasion and to determine what should be done to reassert the right of the individual to be free of Government surveillance.[71]

In his introductory remarks, the Chairman indicated that between 1934 and 1967, 16 sets of Congressional hearings had been held which dealt with wiretapping and electronic eavesdropping.[72] It was noted that the creation of two independent commissions—the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance (P.L. 90–351) and the National Commission on Individual Rights (P.L. 91–452)—would aid in the examination of some of the same issues. The Subcommittee's independent study, according to Rep. Kastenmeier, would perform a valuable oversight function in this sensitive area and would present an immediate response to the problems.

SECURITY AND PRIVACY OF CRIMINAL ARREST RECORDS

In the 92d Congress the House Judiciary Subcommittee no. 4 held hearings in the spring of 1972 on H.R. 13315, which focused on the dissemination and use of criminal arrest records.[73] Representative Don Edwards of California, Subcommittee Chairman, commented on

---

[69] Ibid., p. 61.
[70] U.S. Congress. House. Committee on the Judiciary. Subcommittee on Courts, Civil Liberties, and the Administration of Justice. Wiretrapping and electronic surveillance. Hearings, 93d Congress, 2d session, April 24–29, 1974.
[71] Ibid., p. 1.
[72] Ibid., p. 2.
[73] U.S. Congress. House. Committee on the Judiciary. Subcommittee No. 4. Security and privacy of criminal arrest records. Hearings, 92d Congress, 2d session, March 16–April 26, 1972.

the need to protect criminal arrest records from possible misuse and noted that the protection of these records were a part of the larger issue of privacy and security of criminal justice information. At the opening of these initial hearings, he observed that:

> The narrow scope of our present undertaking is not meant to indicate a lack of concern with other types of information relating to criminal procedures. Rather it reflects the compelling importance of the damage done by arrest records and the belief that this issue can be most effectively dealt with if separated from other issues which are also important.[74]

The hearings highlighted some of the significant aspects of the issue and impact of criminal arrest information systems. Testimony emphasized that arrest records should contain disposition information and that, in the absence of such information, the records might be misinterpreted, causing unnecessary economic and social hardships.

"POSTAL INSPECTION SERVICE'S MONITORING AND CONTROL OF MAIL SURVEILLANCE AND MAIL COVER PROGRAMS"

Oversight reviews of the "Postal Inspection Service's Monitoring and Control of Mail Surveillance and Mail Cover Programs" were conducted by the Subcommittee on Postal Facilities, Mail, and Labor Management of the House Committee on Post Office and Civil Service. Several days of testimony, scheduled from May through November, 1975, examined diverse activities of the Inspection Service—mail covers, mail openings, postal surveillance assistance to the Central Intelligence Agency and other Federal agencies, conflicts with privacy rights of individuals, and controls over Inspection practices. Testimony was provided by the Chief Postal Inspector of the Postal Service, representatives of the Intelligence Division of the FBI, the Criminal Division of the Justice Department, and the Director of the Central Intelligence Agency. The genesis of the specific hearings, according to the Subcommittee chairman, Rep. Charles Wilson, were the revelations concerning illegal mail opening operations:

> If the revelations of the past few years have taught us anything, they have reaffirmed that no man or agency can be above the law, and that the basic rights of the individual must be preserved.
>
> This subcommittee will thoroughly investigate the issues raised by mail surveillance, and then take any necessary legislative action to insure that abridgement of individual rights will not be permissible through the improper official use of his or her mail.[75]

The Subcommittee inquires examined the Postal Service policy surrounding mail covers and mail openings as well as the legal authority supporting surveillance by the Postal Service. One of the critical issues examined was that the actual mail openings were conducted by the CIA, rather than the Postal Service, despite an uncertainty on the part of appropriate Postal Service Inspection officials that the CIA had legal authority to proceed with the operation.[76]

---

[74] Ibid., p. 1.

[75] U.S. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Postal Facilities, Mail, and Labor Management. Postal Inspection Service's Monitoring and Control of Mail Surveillance and Mail Cover Programs. Hearings, 94th Congress, 1st session, May 6–Nov. 5, 1975, p. 2.

[76] Ibid., pp. 11–13 and 59.

"INTERNAL REVENUE SERVICE INTELLIGENCE OPERATIONS"

Hearings held by the Subcommittee on Oversight of the House Committee on Ways and Means examined "Internal Revenue Service Intelligence Operations." Conducted in March and June, 1975, the hearings served the following purposes, as described by Subcommittee Chairman Charles Vanik:

> The hearings will attempt to explore what the IRS is doing in gathering and using intelligence data and how these procedures relate to the legitimate needs of the IRS in administering the tax laws as well as how they affect the basic rights of American citizens.[77]

The questions regarding IRS data gathering and collection focused on the Intelligence Gathering and Retrieval System, a standardized system for organizing material and information collected by the IRS initiated in 1973, and "Operation Leprechaun," an IRS surveillance of 30 prominent Miami, Florida citizens, which involved questionable practices. The concerns of the hearings were that personal and private matters, unrelated to tax requirements, were being investigated by the IRS and that this information, even if erroneous, was maintained by the Service.

"IRS OPERATIONS AND TAXPAYER ASSISTANCE"

In early 1975, the Subcommittee on Oversight of the House Committee on Ways and Means reviewed "IRS Operations and Taxpayer Assistance" with a focus on infomation on delinquent taxpayers, rules governing disclosure of tax information to the White House, and the IGRU/IGRS (the Information Gathering and Research Unit/ the Information Gathering and Retrieval System of IRS).

The IGRS consisted of a District Background Files Index and a National Register. The former included nearly 500,000 names of organizations, individuals, or other entities and was utilized by 45 IRS districts.

The privacy and confidentiality of tax returns was the subject of some questions, especially with regard to access to such returns by Federal agencies. Testimony by IRS officials provided the guidelines which the Service uses in determining whether or not IRS should honor an agency request to inspect certain income tax returns. In response to questions from Subcommittee members, IRS Commissioner Donald Alexander testified that based upon Executive Order 11805, issued by President Ford on Sept. 20, 1974, guidelines and controls have been applied to access to tax returns by the President and White House officials.[78]

"OPERATION LEPRECHAUN"

"Operation Leprechaun," the term applied to certain Internal Revenue Service surveillance and investigations in the Miami, Florida

---

[77] U.S. Congress. House. Committee on Ways and Means. Subcommittee on Oversight. Internal Revenue Service Intelligence Operations. Hearings, 94th Congress, 1st session, March 26 and June 25, 1975, p. 1.

[78] U.S. Congress. House. Committee on Ways and Means. Subcommittee on Oversight. IRS Operations and Taxpayer Assistance. Hearings, 94th Congress, 1st session, Feb. 27 and April 14, 1975, pp. 10–11.

area, generated several days of hearings in the 94th Congress by the Subcommittee on Oversight of the House Committee on Ways and Means. The hearings focused on policies and operations of the Intelligence Division and the Inspection Service of IRS and their purposes were summarized by the Subcommittee chairman, Rep. Charles Vanik:

> The last several years have uncovered the most incredible cases of violations of rights by Federal law enforcement and security agencies. The subcommittee is concerned that such violations not occur in the Internal Revenue Service . . . I am concerned that in the atmosphere of recent allegations, the pendulum may have swung too far against the legitimate role of the IRS as a law enforcement agency . . . I would hope that we could help the IRS develop a policy which provides for full protection of the rights of individuals within a program of vigorous prosecution of criminal tax evasion . . . (and) that obtaining the truth about the real nature of the alleged abuses in some of the Intelligence Division operations the Congress can help in this important debate and provide some policy guidelines.[79]

One of the findings of the hearings was the absence of normal supervisory control by IRS Intelligence Division over such operations and the misuse of certain surveillance techniques and activities.

The hearings also included written responses from the Internal Revenue Service regarding earlier Subcommittee requests. The extensive IRS comments included a description of the Exempt Organizations Master File (EOMF) which numbered more than 690,000 entries in 1975, the authorities and manual guidelines for the use of electronic devices and surveillance by IRS, history and development of the Intelligence Gathering and Retrieval System operated by IRS, and IRS wiretap authority. According to the prepared statement, IRS does not engage in Title III wiretaps (for national security purposes) but only in open tax investigations of Title 18 violations committed in contravention of the internal revenue laws. In that case, only consensual wiretaps (i.e. the consent of one of the parties) may be employed.[80]

"U.S. INTELLIGENCE AGENCIES AND ACTIVITIES"

During the 94th Congress, the House Select Committee on Intelligence conducted inquiries parallel to the Senate Select Committee investigations into alleged abuses by U.S. intelligence agencies. The final report of the Committee has not been released, although a series of recommendations regarding the re-structuring of the intelligence community, its operations, and congressional oversight have been proposed by the Committee.[81] The Select Committee recommendations include, among others, the re-establishment of the National Security Agency as an independent agency with civilian control; the disclosure of a total single sum budgeted for each agency involved in intelligence; that a Director of Central Intelligence be created for the purpose of coordinating and overseeing the entire foreign intelligence community with a view to eliminating duplication in collection and promoting competition in analysis, including a comprehensive inquiry into the causes of intelligence failures, inadequate collection tasking, analytical bias, duplication, unusable technical output, and withholding of in-

---

[79] U.S. Congress. House. Committee on Ways and Means. Subcommittee on Oversight. Operation Leprechaun. Hearings, 94th Congress, 1st session, Dec. 2, 1975, pp. 1–2.
[80] Ibid., p. 199.
[81] U.S. Congress. House. Select Committee on Intelligence. Recommendations of the Final Report. 94th Congress, 2d session, Feb. 11, 1976. House Report No. 94–833.

formation by senior officials; full and complete management and financial audit by the General Accounting Office; increased internal audit staff for the CIA; amending of legislation which restricts the Directors and heads of foreign intelligence agencies from providing full information to the appropriate committees of Congress; abolition of the Defense Intelligence Agency and transfer of functions to Assistant Secretary of Defense for Intelligence and the CIA; that no agency of the United States engaged principally in foreign or military intelligence, directly or indirectly engage in the training or the supplying of domestic police agencies of the United States; that the intelligence components of the armed services of the United States be prohibited from engaging in covert action within the United States; and a series of restrictions of domestic intelligence operations conducted by the FBI and Department of Justice.[82]

In one set of hearings, the House Select Committee focused on domestic intelligence programs of several intelligence agencies.[83] Various units, including the Domestic and International offices of the Drug Enforcement Agency, Intelligence Division of the Federal Bureau of Investigation, and the Investigations and Enforecment support components of the U.S. Customs Service, testified regarding domestic surveillance operations. The inquiry examined the employment of former FBI personnel by American Telephone and Telegraph, specific FBI investigations and surveillances of U.S. citizens and particular groups, authority and surveillance requests surrounding the "Kissinger Wiretaps," and certain FBI record-keeping and information systems, such as the National Crime Information Center containing over six million records relating to various crimes and criminal histories, the Automated Identification Division System with a total number of nearly 1.4 million records, and the Investigative Support Information System.[84]

3. Selected Joint Committee Document

"Investigation of the Special Service Staff of the Internal Revenue Service"

The Staff of the Joint Committee on Internal Revenue Taxation prepared a report on the "Investigation of the Special Service Staff of the Internal Revenue Service," released on June 5, 1975. Among other items, the examination reviewed files generated by the Special Service Staff (SSS), the information received by the SSS from other Federal agencies and State and local government units, and transmittal of such information to the White House and Federal agencies, and the concentration of SSS efforts on Vietnam war tax resisters, "ideological organizations," and "extremist" organizations. The staff investigation into the SSS discovered that its files on individuals and organizations were supplemented by FBI lists and information, the Inter-Divisional Information Unit (IDIU) in the Justice Department, and other Federal agencies. IDIU provided the Special Service Staff

[82] Ibid. passim.
[83] U.S. Congress. House. Select Committee on Intelligence. U.S. Intelligence Agencies and Activities: Domestic Intelligence Programs. Hearings, 94th Congress, 1st session, Oct. 9–Dec. 10, 1975.
[84] Ibid. passim.

with its computerized alphabetical list of individuals involved in civil disturbances, at one point numbering 16,000. The SSS files numbered nearly 11,500 at their peak.

The Joint Committee staff examination of the SSS files found a lack of standard criteria governing their development or utilization, incorporation of information which was not evaluated or screened, and the concentrated accumulation of information on political activities. The staff report concluded that . . .

> While the Revenue Service must accumulate information on individuals and organizations to properly carry out its taxing function, a basic question raised because of SSS activity is whether the IRS should ever accumulate information on the political activities of organizations or individuals.[85]

Summary of Section B. Compendium of Congressional Related Materials

This section contains the following items:

1. EXCERPTS FROM CONGRESSIONAL DOCUMENTS

U.S. Congress. House. Committee on Government Operations. The use of polygraphs and similar devices by Federal agencies. Report. 94th Congress, 2d session. Jan. 28, 1976. House Report no. 94–795.

U.S. Congress. House. Republican Task Force on Privacy. Recommendations. 93d Congress, 2d session. August 21, 1974. Included in remarks of Hon. Barry M. Goldwater, Jr. Congressional Record, v. 120, September 12, 1974: H9234–H9238.

U.S. Congress. Senate. Committee on Aeronautical and Space Sciences. Space benefits—the secondary application of aerospace technology in other sectors of the economy. 94th Congress, 1st session. April 16, 1975. pp. 30–31.
(At head of title: committee print).

U.S. Congress. Senate. Committee on Armed Services. Special Electronic Battlefield Subcommittee of the Preparedness Investigating Subcommittee. Investigation into electronic battle field program. Report. 92d Congress, 1st session. Feb. 22, 1971. pp. iii, 1–3, and 18–20.
(At head of title: committee print).

2. GENERAL ACCOUNTING OFFICE REPORTS

U.S. General Accounting Office. Development of the computerized criminal history information system. Letter report and enclosure to Hon. Sam J. Ervin, Jr., Chairman, Subcommittee on Constitutional Rights, Senate Committee on the Judiciary. March 1974. (B–171019) pp. 1–10.

U.S. General Accounting Office. FBI domestic intelligence operations—their purpose and scope: issues that need to be resolved. Feb 24, 1976. (GGD–76–50). pp. i–xviii.

---

[85] U.S. Congress. Joint Committee on Internal Revenue Taxation. Investigation of the Special Service Staff of the Internal Revenue Service. Report prepared by the Joint Committee staff. 94th Congress, 1st session, June 5, 1975. (Committee print), p. 111.

3. CONGRESSIONAL RESEARCH SERVICE REPORTS

U.S. Library of Congress. Computer and information security in the Federal government: an overview. Memorandum by Louise Giovane Becker to Hon. Abraham Ribicoff, Chairman, Senate Committee on Government Operations. U.S. Congress. Senate. Committee on Government Operation. Problems associated with computer technology in Federal programs and private industry: computer abuses. 94th Congress, 2d session. June 1976. pp. 153–161.
(At head of title: committee print)

U.S. Library of Congress. Congressional oversight of intelligence: status and recommendations. Multilith prepared by Frederick M. Kaiser, no. 76–54 G. March 11, 1976. 50 p.

U.S. Library of Congress. Wiretapping and electronic surveillance: Federal and state laws. Multilith prepared by Christopher M. Wasi, M. Elizabeth Smith, and Charles Doyle, no. 74–140 A. July 25, 1974. pp. i, 1–37.

Union Calendar No. 392

94th Congress, 2d Session - - - - - - - House Report No. 94-795

THE USE OF POLYGRAPHS AND SIMILAR DEVICES BY FEDERAL AGENCIES

THIRTEENTH REPORT

BY THE

COMMITTEE ON GOVERNMENT OPERATIONS

together with

SEPARATE AND DISSENTING VIEWS

JANUARY 28, 1976.—Committeed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE

57-006 WASHINGTON : 1976

COMMITTEE ON GOVERNMENT OPERATIONS

JACK BROOKS, Texas, *Chairman*

L. H. FOUNTAIN, North Carolina
JOHN E. MOSS, California
DANTE B. FASCELL, Florida
TORBERT H. MACDONALD, Massachusetts
WILLIAM S. MOORHEAD, Pennsylvania
WM. J. RANDALL, Missouri
BENJAMIN S. ROSENTHAL, New York
JIM WRIGHT, Texas
FERNAND J. ST GERMAIN, Rhode Island
FLOYD V. HICKS, Washington
DON FUQUA, Florida
JOHN CONYERS, Jr., Michigan
BELLA S. ABZUG, New York
JAMES V. STANTON, Ohio
LEO J. RYAN, California
CARDISS COLLINS, Illinois
JOHN L. BURTON, California
RICHARDSON PREYER, North Carolina
MICHAEL HARRINGTON, Massachusetts
ROBERT F. DRINAN, Massachusetts
EDWARD MEZVINSKY, Iowa
BARBARA JORDAN, Texas
GLENN ENGLISH, Oklahoma
ELLIOTT H. LEVITAS, Georgia
DAVID W. EVANS, Indiana
ANTHONY MOFFETT, Connecticut
ANDREW MAGUIRE, New Jersey
LES ASPIN, Wisconsin

FRANK HORTON, New York
JOHN N. ERLENBORN, Illinois
JOHN W. WYDLER, New York
CLARENCE J. BROWN, Ohio
GILBERT GUDE, Maryland
PAUL N. McCLOSKEY, Jr., California
SAM STEIGER, Arizona
GARRY BROWN, Michigan
CHARLES THONE, Nebraska
ALAN STEELMAN, Texas
JOEL PRITCHARD, Washington
EDWIN B. FORSYTHE, New Jersey
ROBERT W. KASTEN, Jr., Wisconsin
WILLIS D. GRADISON, Jr., Ohio

WILLIAM M. JONES, *General Counsel*
JOHN E. MOORE, *Staff Administrator*
WILLIAM H. COPENHAVER, *Associate Counsel*
LYNNE HIGGINBOTHAM, *Clerk*
J. P. CARLSON, *Minority Counsel*

GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS SUBCOMMITTEE

BELLA S. ABZUG, New York, *Chairwoman*

LEO J. RYAN, California
JOHN CONYERS, Jr., Michigan
TORBERT H. MACDONALD, Massachusetts
JOHN E. MOSS, California
MICHAEL HARRINGTON, Massachusetts
ANDREW MAGUIRE, New Jersey
ANTHONY MOFFETT, Connecticut

SAM STEIGER, Arizona
CLARENCE J. BROWN, Ohio
PAUL N. McCLOSKEY, Jr., California

TIMOTHY H. INGRAM, *Staff Director*
ERIC L. HIRSCHHORN, *Counsel*
ROBERT FINK, *Professional Staff Member*
THEODORE J. JACOBS, *Professional Staff Member*
WILLIAM G. FLORENCE, *Professional Staff Member*
RUTH MATTHEWS, *Professional Staff Member*
ANITA WIESMAN, *Clerk*

LETTER OF TRANSMITTAL

HOUSE OF REPRESENTATIVES,
Washington, D.C., January 28, 1976.

Hon. CARL ALBERT,
Speaker of the House of Representatives,
Washington, D.C.

DEAR MR. SPEAKER: By direction of the Committee on Government Opertations, I submit herewith the committee's thirteenth report to the 94th Congress. The committee's report is based on a study made by its Government Information and Individual Rights Subcommittee.

JACK BROOKS, *Chairman.*

CONTENTS

	Page
I. Introduction	1
II. Background	4
Polygraph	4
Psychological stress evaluator	5
Voice analyzer	6
Other devices and techniques	6
III. Research and the fallibility of "lie detector" devices	8
Federally funded research—polygraphs	8
Federally funded research—voice analyzers	10
Proposed federally funded research—polygraphs	11
American Polygraph Association research	12
Continued need for definitive research	12
IV. Legal and moral considerations	15
"Lie detectors" and constitutional safeguards	15
The "right to prove one's innocence"	16
Admissibility in evidence	17
Justice Department position on admissibility	17
V. Policy and standards established by the Civil Service Commission	20
Current Civil Service Commission regulations	20
Commission's assessment of agency polygraph use	22
VI. Ownership and use of "lie detectors" by Federal agencies	25
Financial and statistical data	25
Use of psychological stress evaluator	27
Use of voice analyzers	29
Intelligence agency practices differ	29
Does the intelligence community rely too heavily on polygraph testing?	30
VII. Polygraph operators and the quest for professionalism	32
Current criteria for selection of examiners	32
Polygraph examiner training	33
Department of Defense training	33
Other agency training of examiners	34
Efforts toward professionalism	35
VIII. The polygraph test and safeguards for the individual	38
Who authorizes tests?	39
Consideration of physical and mental condition	40
Weight accorded polygraph tests	41
Effect of refusals to be polygraphed	42
Availability of results to individuals tested	43
Assurance of confidentiality of test results	44
Appeals of polygraph test results	45
Special test facilities	45
IX. Recommendations	46

APPENDIXES

Appendix A.—Questionnaire on polygraphs and psychological stress evaluators	47
Appendix B.—Correspondence from former Chairman Moorhead to the Executive Secretary of the President's Foreign Intelligence Advisory Board	49
Appendix C.—Correspondence from the Executive Secretary of the President's Foreign Intelligence Advisory Board to former Chairman Moorhead	50

VI

Separate views of Hon. Sam Steiger (concurred in by Hon. Frank Horton, Hon. John N. Erlenborn, Hon. John W. Wydler, Hon. Clarence J. Brown, Hon. Garry Brown, Hon. Charles Thone, Hon. Edwin B. Forsythe, and Hon. Elliott H. Levitas)---------- Page 51
Dissenting views of Hon. Frank Horton, Hon. Clarence J. Brown, Hon. Paul N. McCloskey, Jr., Hon. Joel Pritchard, Hon. John N. Erlenborn, Hon. Charles Thone, Hon. Garry Brown, Hon. Edwin B. Forsythe, Hon. Alan Steelman, Hon. Robert W. Kasten, Jr., Hon. Sam Steiger, Hon. John W. Wydler, and Hon. Willis D. Gradison, Jr----------

Union Calendar No. 392

94TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT
2d Session } { No. 94-795

THE USE OF POLYGRAPHS AND SIMILAR DEVICES BY FEDERAL AGENCIES

JANUARY 28, 1976.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

THIRTEENTH REPORT

together with

SEPARATE AND DISSENTING VIEWS

BASED ON A STUDY BY THE GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS SUBCOMMITTEE

On January 22, 1976, the Committee on Government Operations approved and adopted a report entitled "The Use of Polygraphs and Similar Devices by Federal Agencies." The chairman was directed to transmit a copy to the Speaker of the House.

I. INTRODUCTION

In 1964, the Foreign Operations and Government Information Subcommittee made its initial study of the Federal Government's use of polygraphs as "lie detectors." Over the years, such use of polygraphs had become an increasingly controversial topic. As a consequence, both public officials and private citizens were raising serious questions regarding the propriety of their use, as well as the validity and reliability of such devices. Consultation with the Library of Congress disclosed that no study of the Federal Government's use of polygraphs had ever been made by the Congress, by any agency of the executive branch, or by private researchers.

On the basis of hearings conducted in 1964, a report entitled "Use of Polygraphs as 'Lie Detectors' by the Federal Government" was issued by the Committee on Government Operations in March 1965. It concluded that:

> There is no "lie detector," neither machine nor human. People have been deceived by a myth that a metal box in the hands of an investigator can detect truth or falsehood.[1]

[1] H. Rept. 89-198, p. 1.

The committee expressed its concern that this myth was being encouraged by substantial Federal Government expenditures for polygraph machines and on salaries for hundreds of Federal investigators who were conducting thousands of polygraph examinations. To correct the obvious defects and to protect employees from abuse in connection with polygraph examinations, the committee recommended that the Federal Government:

> Initiate comprehensive research to determine the validity and reliability of polygraph examinations.
>
> Prohibit the use of polygraphs in all but the most serious national security and criminal cases.
>
> Improve the training and qualifications of Federal polygraph operators.
>
> Restrict the use of two-way mirrors and recording devices during polygraph examinations.
>
> Guarantee that polygraph examinations be, in fact, voluntary.
>
> Insure that refusal to take a polygraph examination will not constitute prejudice or be made a part of an individual's records except in the most serious national security cases.[2]

The committee also recommended that the President immediately establish an interagency committee to study problems posed by the Federal Government's use of polygraphs and to work out solutions to those problems.

Four months after that report by the committee, the Department of Defense issued a comprehensive directive to regulate the conduct of polygraph examinations and to improve the selection, training, and supervision of its polygraph operators.

A subsequent report by the committee dated September 26, 1966,[3] commented both on the directive issued by the Department of Defense and on the establishment of an Interagency Polygraph Committee by President Lyndon B. Johnson in November 1965. The directive was recognized in the report as the first step taken by any Federal agency to curtail the widespread use of so-called "lie detectors." Its provisions for stricter controls and for research were considered to be in harmony with most of the recommendations previously made by the committee. The Department of Defense directive, however, did not respond fully to the recommendation that the Federal Government prohibit the use of polygraphs in all but the most serious national security and criminal cases.

The interagency group's detailed study of the overall utilization of polygraph machines throughout the executive branch was then still in process, and the final report was not available to the committee for evaluation. This committee did, however, include the following recommendations in its own September 1966, report:

> 1. The Department of Defense polygraph directive is a good first step forward. But now a second should be taken. The Department should immediately reconsider the permissive use of the device for pre-employment screening with the

---

[2] Ibid., p. 2.

[3] "Use of Polygraphs as 'Lie Detectors' by the Federal Government" (pt. 2), H. Rept. 89–2081.

view of fulfilling the committee's recommendation to prohibit the use of polygraphs in all cases but those clearly involving the Nation's security.

2. Qualified physicians and psychiatrists should be included among the appropriate supervisory officials designated to review polygraph examination records.

3. All Government agencies should be placed under a uniform administrative system which will enforce maximum controls on the use of polygraphs, and which will establish regulations to prevent their proliferation and misuse.[4]

In June of 1974, the Foreign Operations and Government Information Subcommittee held hearings to update its information on this subject.[5] Not only had nearly a decade passed since the previous hearings but new technology and techniques have been developed.

The subcommittee used a questionnaire [6] in addition to public hearings, as it did in its earlier inquiry, to develop the data and views included in this report.

---

[4] Ibid., p. 4.
[5] "The Use of Polygraphs and Similar Devices by Federal Agencies." Hearings before a subcommittee of the Committee on Government Operations, House of Representatives, June 4 and 5, 1974.
[6] Appendix A, p. 47.

II. BACKGROUND

History is full of instances where different cultures and societies have attempted to detect lies and verify truth. Some of the ancient tests reflected a primitive understanding of psychology or physiology, but they were hardly reliable or scientific. They had in common a significant dependence on brutality, deception, or chance as the determinant of guilt or innocence.

At various times, and in different places, there evolved such tests as the ordeal of boiling water, the ordeal of the red hot iron, and the ordeal of the red hot stones. In one such ordeal, a suspected wrongdoer was required to thrust his hand into a fire. If the hand was unsinged when removed, the individual was declared innocent; if the hand was burned, that was positive proof of guilt. In other circumstances, truth or lack of truth might be determined by the pattern assumed by a handful of tossed pebbles. A test used by the early Chinese required suspects to chew rice powder while being questioned. If the rice powder was dry when spit out, the man was condemned, on the premise that the tension of guilt supposedly dried up his salivary glands.

Modern criminology is more sophisticated, and utilizes a wide variety of devices and methods which have been developed to assist in apprehending suspected criminals and establishing their guilt or innocence. Among those generally acceptable to the courts [7] as admissible evidence are the results of tests relating to fingerprinting, ballistics, and handwriting. Others, such as the results of polygraph tests, have not yet merited that "general acceptance."

Polygraph

The polygraph concept presumes that an identifiable physical reaction can be attributed to a specific emotional stimulus. Erasistratus, a Greek physician and anatomist of the third century B.C., reported that emotion caused a quickening of the pulse, but the first attempt to use a scientific instrument as an aid in detecting lies dates back to 1895 when Cesare Lombroso, an Italian criminologist, claimed success in determining the guilt or innocence of suspected criminals by noting whether their blood pressure or pulse changed during interrogation.

In a book entitled "On the Witness Stand" published in 1908, Harvard psychology professor Hugo Munsterberg discussed possibilities of detecting lies by recording physiological changes. Changes in breathing rates were linked to attempts at deception by another Italian

[7] In *Frye* v. *United States* (293 F. 1013 [D.C. Cir. 1923]) the court made the following observation relative to the general acceptance test of admissibility: "Just when a scientific principle or discovery crosses the line between the experimental and demonstrable stages is difficult to define. Somewhere in this twilight zone the evidential force of the principle must be recognized and while courts will go a long way in admitting expert testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs."

criminologist, Vittorio Benussi, in 1914. The following year William Moulton Marston, a criminal lawyer and student of Munsterberg, began systematic research at the Harvard Psychological Laboratory into the correlation between lying and changes in blood pressure.

During World War I, Marston headed a committee of psychologists formed by the National Research Council to look into the known deception tests and report on their possible usefulness in counter-intelligence activities. Using a sphygmomanometer, the device physicians use to measure a patient's blood pressure, Marston conducted experiments by taking intermittent readings of blood pressure during interrogation periods. After performing a number of experiments, the committee of psychologists concluded that the Marston blood pressure test was 97 percent reliable. It recommended that Marston be appointed Special Assistant to the Secretary of War with authority to use his method in spy cases. War Secretary Newton D. Baker took no action on the recommendation, but the committee's work aroused the interest of a young psychologist, John A. Larson, who was connected with the Berkeley, Calif., police force.

In 1921 Larson devised an instrument capable of simultaneously recording blood pressure, pulse rates, and respiratory changes, the forerunner of today's polygraph. Working under Berkeley Police Chief August Vollmer, sometimes called the father of scientific police work in this country, Larson used his device with reported success on hundreds of criminal suspects. Presently he was joined on the Berkeley force by a young man named Leonarde Keeler.

Keeler, a Stanford University psychology major, was destined to become the best known expert in the field. In 1926, he developed an improvement of Larson's apparatus. Keeler continued refining his device, which he named the Keeler polygraph, and incorporated into it the feature of measuring changes in the skin's resistance, commonly known as "galvanic skin respone." He also developed polygraph interrogation techniques while at the scientific crime detection laboratory at Northwestern University from 1930 until 1938, when he entered private business.

The term polygraph refers, most precisely, to the multiple-pen subsystem which records the instrumental responses on a roll of paper: through usage, it has come to represent the entire lie detection equipment. Contemporary polygraph equipment measures simultaneously three physiological responses:

Physiological response	Device	Method of sensing
Breathing pattern	Pneumograph	Corrugated rubber tube around chest.
Blood pressure and pulse	Cardio-sphygmomanometer	Pneumatic pressure cuff around upper arm (or around wrist and forearm to minimize discomfort)
Skin resistance to external current	Psycho-galvanometer	Finger or palmar surface electrodes.

Psychological Stress Evaluator

The psychological stress evaluator (PSE–1) was developed by two retired Army intelligence personnel and has been marketed by them through Dektor Counterintelligence & Security, Inc., of Springfield, Va., since 1970. The instrument capitailzes on the principle of in-

voluntary physiological changes that are related to psychological stress. It is designed to measure and to graphically display certain stress-related components of the human voice's two modulations—the audible and the inaudible.

According to the developers of the PSE–1, there are inaudible frequency modulations in speech that are superimposed on those audible modulations of the voice that are heard. They further represent that the internal stresses which are reflected in those inaudible variations of the voice are not totally controlled by the brain or thought processes, and that those variations can be detected and recorded by their PSE–1 device.

Two significant advantages are claimed for the PSE–1 over other types of "lie detector" devices. First is its simplicity, in that it has relatively few moving parts and it is relatively easy to learn to operate. Second, the PSE–1 does not have to be used at the time of the interview or interrogation. A tape recorder is used to make a permanent record of the interview, and the tape is later fed into the PSE–1 and the voice reactions recorded on a chart. Users of the device frequently make tape recordings for clients over the telephone, run the tape on the PSE–1, and report the test results to their clients.

Voice Analyzer

Research on the capability of a speech parameter to differentiate truthful from deceitful responses, by measurement of the energy changes in the lower and mid-range speech frequencies, begun in 1963 by Mr. Fred Fuller, culminated in 1970 in the development of the voice stress analyzer. The acknowledged shortcomings of that instrument by its developer led to further research of those rapid variations in the tremolo or vibrato amplitude of speech. In 1972, a second device known as the Mark II voice analyzer was introduced by this same individual. That device electronically extracts a numerical value of those rapid variations in the tremolo or vibrato amplitude of speech, which the developer represents varies with changes in emotional stress.

The Mark II voice analyzer and the Dektor psychological stress evaluator both use the analysis of speech as a basis for inferring truth or deception. They are, however, two completely different instruments and the features extracted from speech for measurement by these instruments are entirely different. The developer of the Mark II voice analyzer claims that because it shows an instantaneous numerical value reading, it provides the most rapid means of detecting deception and the most precise indication of emotional reaction of any instrument.

Other Devices and Techniques

A 1962 report by the Institute for Defense Analysis, cited in the subcommittee's earlier hearings,[8] notes that suggestions have been made that other physiological responses, such as face temperature, electrocardiograph and electro-encephalograph should be included in lie de-

[8] Hearings, subcommittee of the Committee on Government Operations, House of Representatives, 88th Cong., 2d sess., Apr. 29 and 30, 1964. "Use of Polygraphs as 'Lie Detectors' by the Federal Government—Panel Discussion with Scientists," (pt. 3), pp. 425–463.

tection work but virtually no research had been done to learn whether the addition of these indicators would increase the accuracy of lie detection.

Dr. Frederick Davidson, a professor at Kent State University in Ohio, claims to have discovered a lie detection technique that works on a subject who never opens his mouth.[9] Dr. Davidson reports that he merely examines change in retina color, plus change in pupil size and in eye focus, to determine emotional response to stimuli-like questioning. Thus, he says, the conventional retinoscope can become a lie detector. It allegedly works, too, on an intoxicated or drugged individual because it measures responses in the eye's retina to questions or comments. The method was used temporarily to screen applicants for campus police jobs at Kent State University.

The Weizmann Institute of Rehovot, Israel, recently reported development of a "microwave respiration monitor" to determine truthfullness remotely and without the knowledge of the subject.[10] This device, presently being used in addition to the polygraph by the Israeli police, measures the palpitations of the stomach by use of a microwave. The theory is that lying produces an increased rate of respiration which can be detected by increased movement of the stomach. The device offers the possibility of widespread, random, remote and surreptitious "truth verification" at border crossings, airports, and police lineups. The developers hope to market the device in the United States shortly.

---

[9] Hearings, pp. 113–120. See footnote 5 on p. 3.
[10] Hearings, pp. 121–140. See footnote 5 on p. 3.

III. RESEARCH AND THE FALLIBILITY OF "LIE DETECTOR" DEVICES

No body of empirical scientific data existed 10 years ago to demonstrate that the polygraph was either valid or reliable, or both, when used as an instrument for lie detection. The subcommittee found that Federal investigators had given thousands upon thousands of polygraph tests, but that there had been no attempt to determine the validity of the procedure and no attempt to find out whether the polygraph operator really could detect falsehoods. No statistical proof had been compiled, despite thousands of cases; no scientific proof had been produced, despite thousands of opportunities.

The need for and importance of research were highlighted to the subcommittee by the views expressed by many expert witnesses that lie detection tests could be rendered nearly or completely invalid. This could occur if the physical or mental makeup of the individuals being tested involved extreme nervousness, physiological abnormalities, mental abnormalities; if there was a lack of or managed emotional response; and if bodily movements were undetected. These and other factors make it possible for an individual to mislead examiners. Moreover, in the view of those experts, polygraph examiners had neither the training nor ability to recognize obscure mental or emotional abnormalities.

For that reason, the committee's first recommendation in its earlier report was that:

> The Federal Government initiate comprehensive research to determine the validity of polygraph examinations.

Federally Funded Research—Polygraphs

A DOD joint services group on polygraph research, established shortly thereafter to act on that recommendation, developed a research program which contemplated six studies:

a. Evaluation of basic instrumentation now employed in polygraph examinations for the assessment of the reliability and adequacy of measurement of the physiological changes assumed to be significant. The test standards and methods for this purpose will be established by an unbiased agency, the National Bureau of Standards.

b. An extensive field test of the reliability of polygraph field instrumentation in use.

c. A study of the reliability of examiners in polygraph chart interpretation.

d. An attempt to establish external criteria in criminal cases which will make it possible to perform studies of the validity of each aspect of the polygraph examination.

e. An examination of the possibilities inherent in modern instrumentation and computer data processing in the assessment of physiological changes.

f. Collection and analysis of descriptive statistics on polygraph operations.

The Air Force provided $200,000 in October 1966 to support this program, designated as Project 4356, at Rome Air Development Center. Earlier, the Air Force transferred $16,500 to the Navy for a contract to the National Bureau of Standards to evaluate the response characteristics of two standard polygraph instruments. A total of $111,516 was actually spent, with $104,984 reserved for studies awaiting approval. Although a continuing program of research was contemplated, no funds were provided in fiscal year 1968.

The major reason for research planned and undertaken on the polygraph was to determine its validity, more commonly called accuracy. Validity is defined as a measure of the agreement between the results of a polygraph examination in the absence of any other information and some independent and acceptable way of establishing a person's true guilt or innocence. Validity should be distinguished from reliability. Reliability is simply a measure of agreement between two or more examiners on the same case (or between two tests by the same examiner) ; i.e., it is a measure of consistency.

Unfortunately, it is possible to be both consistent and wrong. On the other hand, high accuracy is not possible if reliability is low. Validity, i.e., agreement of a polygraph examination with "the truth" (as measured in a test program) is, obviously, the central issue concerning the value of the polygraph as a test of deception in routine use.

The joint services group recognized that it is relatively easy to measure the validity of the polygraph in a laboratory because steps can be taken to insure precise knowledge of the subject's "guilt" or "innocence" and to insure independent judgments by the polygraph examiners. As an example, a subject is told to select a particular card from a deck and to respond with the word "No" to all questions about it or any other card. The experimenter can keep the card while the polygraph examiner's task is to determine the subject's choice solely on the basis of the polygraph test.

A more complicated laboratory test of validity is to contrive the subject's participation in some simulated crime, like acting as if he stole a book from a college bookstore, or perhaps even to steal a book (while arrangements have been made for the bookstore manager to look the other way). Experiments of this sort are not regarded as conclusive because, it can be said, the subject does not have a real motive to deceive the examiner, or does not exhibit the same emotions as that of a guilty person in an actual crime. Thus, even though the "laboratory" experiment offers precise control and knowledge of events, some observers do not accept the results of such experiments.

The joint services group was able to accomplish only part of its assignment. It developed a research and development program which, if carried out, was believed capable of establishing the reliability and validity of the polygraph as a means of judging deception. However,

that group was not able to undertake its proposed validation studies because of concern with the possibility of severe adverse reaction on the part of Congress, the press, and the public to that program.[11] Moreover, its proposed TV study of the complete polygraph interrogation could not be undertaken because too few polygraph examinations were being conducted at the time to permit the collection of the required research data in a reasonable amount of time.

The joint services group summarized the results of its curtailed research efforts in an internal report dated August 28, 1968, entitled, "Present Status of DOD Research on the Polygraph." [12] That report states that the joint services group was able to formulate but not to carry out a research program to determine the reliability and validity of a polygraph examination, observing that the conceptual problems of devising a research strategy were less formidable than the practical ones.

Notwithstanding the problems encountered, and the fact that its research program was not completed, the joint services group did reach some conclusions. Paramount was its conclusion that the polygraph remains in use although no steps were being taken to establish its validity. In addition, it concluded that the standard polygraph device is not a precision instrument, and that the response characteristics of the two standard polygraph instruments—Keeler and Stoelting—differ. Moreover, it found that some polygraphs in routine use in the Department of Defense did not perform in accordance with pertinent specifications. The joint services group also noted that, although rather easy to carry out, surprisingly few studies had been accomplished on the reliability of an entire polygraph examination or of any of its parts such as the pre-interrogation interview, type and sequence of questions used in the examination, and chart reading.

The Department of Justice witness, commenting on the matter of the fallibility of polygraph test results, enumerated many reasons [13] for that Department's decision to view such examinations with caution and to oppose their introduction into evidence at trial. Among them was the statement that:

> * * * the results of polygraph examinations cannot be viewed with the same equanimity as the results of forensic tests such as fingerprints, ballistics, and blood tests because * * *.

followed by an enumeration of nine reasons for that view. (See pages 17 through 19 for additional detail.)

Federally Funded Research—Voice Analyzers

With the passage of time, polygraph proponents appear to have accepted without serious question the validity of their device as an instrument for differentiating between truth and deception. They are now increasingly addressing their efforts to demonstrating the reliability of polygraph test results (i.e., consistency in reaching an identical conclusion). Moreover, they no longer give as much emphasis to the term "lie detection" as they used to; instead, they speak of their

[11] Hearings, pp. 630–631. See footnote 5 on p. 3.
[12] Retained in subcommittee files.
[13] Hearings, p. 414. See footnote 5 on p. 3.

testing processes as a means of identifying and measuring changes in stress which are indications of the truth or deception of the answers being given.

The primary strategy and efforts of the proponents of the psychological stress evaluator and the voice analyzers are devoted to demonstrating that, in similar circumstances, their devices are at least as, if not more, reliable than are polygraphs.

In the most recently reported pertinent research, "Comparison of Voice Analysis and Polygraph as Lie Detection Procedures," [14] the researcher's finding was that there existed a clear inferiority of voice analysis, in its present state of development, not only to the polygraph, but also to judgments made on the basis of simply observing subjects' behavior. In view of this, the study concluded that neither of the presently existing voice analysis instruments (i.e., psychological stress evaluator or the voice stress analyzer) warranted acceptance as valid "lie detectors" within the constraint of an experimental paradigm. The CIA, which has been interested in voice analysis for several years does not believe that research to date has been either exhaustive or conclusive, and has plans for research of its own.

Proposed Federally Funded Research—Polygraphs

The subcommittee was advised in May 1974,[15] that the Law Enforcement Assistance Administration (LEAA), of the Department of Justice, had under consideration funding an 18-month study, for approximately $100,000, entitled "Validity and Reliability of Detection of Deception," to consider the following five areas:

1. The basic validity and reliability of polygraph examinations in detecting truth and deception with criminal suspects;
2. The relative effectiveness of various physiological measures, including the currently used standard measures (respiration, skin resistance, cardiovascular activity) and other promising measures which require additional laboratory research;
3. A general evaluation of present practices among field examiners in private practice and in law enforcement settings;
4. The extent to which subject variables such as psychopathy and personality factors influence the effectiveness of the polygraph technique; and
5. The sources of errors in polygraph examinations.

The study is expected to result in reports written for two different audiences. First, a comprehensive and detailed report of the overall research, methodology, results, and conclusions will be prepared, along with individual reports covering each of the five research areas stated above, for those with a scientific and professional interest in the polygraph technique. Secondly, a summary report will be prepared that will give the basic findings and interpret them in terms designed for the criminal justice practitioner who is interested in the problems of application of the polygraph technique.

---

[14] Technical Report No. LWL–CR–03B70, by Joseph F. Kubis, Fordham University, to U.S. Army Land Warfare Laboratory, Aberdeen Proving Ground, Md., 20015—(Final Report Contract No. DAAD05–72–C–0217).

[15] Letter dated May 29, 1974, retained in subcommittee files.

12

American Polygraph Association Research

The level of research directly funded or sponsored by the American Polygraph Association can best be described by that organization's own language—"minimal." [16] Only nominal funds have been allotted to the APA Research and Instrumentation Committee for in-house volunteer efforts concerned mostly with instrumentation and refinement of techniques. These projects receive advance approval by the APA president.

The APA spokesmen were queried, also, concerning the degree to which the organization had itself conducted tests comparing the accuracy and validity of polygraphs and those newer devices which depend primarily on voice analysis. Such a test was reported to have been underway for about a year, conducted by the APA Research and Instrumentation Committee, but no report thereon was expected before August 1974. On March 19, 1975, the subcommittee was advised that this test was suspended, without preparation and issuance of a final report, because of indicated unreliabilities of the PSE equipment being used in the research project.[17]

Continued Need for Definitive Research

When the committee earlier identified the need for and recommended research, it was hopeful that with the passage of some reasonable period of time, some of its doubts and reservations about the validity and reliability of polygraphs might be allayed by the result of that research. However, the nature of research undertaken, both federally and privately funded, and the results therefrom have done little to persuade the committee that polygraphs, psychological stress evaluators, or voice stress analyzers have demonstrated either their validity or reliability in differentiating between truth and deception, other than possibly in a laboratory situation. It is not alone in this view.

The Law Enforcement Assistance Administration of the Department of Justice responded to the subcommittee's request for evaluative information relating to past and recent research on the validity and reliability of polygraphs as follows:

> It has been established that psycho-physiological recordings can be effective in differentiating between truth and deception in mock crime situations in the laboratory, and that the accuracy rate of detection can be manipulated by controlling such variables as age, relevance of the question, degree of motivation of the subject, the number and type of physiological measures being monitored, the number of times the questions are asked, etc.
>
> However, the effectiveness of the lie detection technique when it is used on criminal suspects outside of the laboratory has never been adequately resolved; there is, therefore, a conspicuous lack of reliable data on this point. Polygraph examiners have consistently claimed an error rate of less than one or two percent. Unfortunately, their claims are unsubstantiated, and their statistics were based upon total

[16] Hearings, p. 160. See footnote 5 on p. 3.
[17] Memorandum retained in subcommittee files.

cases rather than confirmed cases. Several scientists have examined criminal suspects, and they have unanimously reported accuracies of essentially 100%. However, they did not publish many details to support their claims.[18]

The Department of Justice was also queried about the justification for underwriting, at a cost of $100,000, the unsolicited research proposal from Dr. David C. Raskin of the University of Utah, in light of the earlier substantial Federal funding of several Department of Defense research projects.

The response to that question again emphasized the significant difference between test results obtained in a laboratory situation and those obtained in a "real life" situation:

> During the last 50 years there have been over 75 laboratory experiments which have indicated that psycho-physiological measurements can greatly increase the probability of determining whether a subject is lying or not. Unfortunately, there are numerous differences between the detection of deception in a laboratory environment and lie detection with criminal suspects. Some of these differences, such as the degree of emotional involvement which the subject has in the outcome of the examination, are obvious and compelling; other differences are more subtle. Some of these differences favor accuracy with criminal suspects. The qualifications, experience and testing techniques of the scientists were not at all representative of lie detection as it is being practiced today. Perhaps the major reason for this is that very few scientists have been trained in current lie detection practices.
>
> Since polygraphs are being used more frequently in the judicial process and are used by the Federal Government, as well as most major law enforcement agencies at State and local levels, it is extremely important that adequate information be available regarding the basic reliability and validity of the techniques. In addition, information is needed about the ways in which the techniques can be improved and the extent to which available techniques are properly employed in present practice. It is the basic purpose of the proposed research by the University of Utah to fill some of the gaps in knowledge concerning those fundamental problems.[19]

The Central Intelligence Agency made similar observations in its testimony before the subcommittee:

> Reliability, defined as consistency of interpretation of polygraph charts, has been looked at by means of examiner agreement studies. Agreement figures from our studies are comparable to figures from similar studies of other groups interpreting data germane to their specialties.
>
> On the other hand, validity—or the degree to which polygraph charts measure what they purport to measure—has been a more difficult issue to evaluate. Satisfactory independent criteria for validating real life conditions are scarce,

[18] Hearings, pp. 638–639. See footnote 5 on p. 3.
[19] Hearings, p. 639. See footnote 5 on p. 3.

and the differences in polygraph subject attitudes between real life and laboratory conditions have prevented much headway through laboratory experiments. The data so far available have not been disappointing, but they are limited, and we still lack an appropriate scientific base for any conclusions.[20]

[20] Hearings, pp. 646–647. See footnote 5 on p. 3.

IV. LEGAL AND MORAL CONSIDERATIONS

The subcommittee heard considerable testimony that the examinaiton of individuals by polygraph or other "lie-detection" instruments infringes on essential individual liberties and protections guaranteed by the Constitution.

"Lie Detectors" and Constitutional Safeguards

The American Civil Liberties Union witness stated that no individual should be required, by moral or legal compulsion, to submit to a "lie detector" test and argued that a number of the Bill of Rights amendments to the Constitution are violated by such a testing procedure. He called further attention to the fact that some European countries have long rejected the polygraph as an impermissible police technique, not so much because of its possibilities for error, but because it was deemed to violate the essential dignity of the human personality and the individuality of a citizen.[21]

The spokesman for the American Federation of Government Employees (AFGE), an organization representing 650,000 Federal employees in exclusive recognition units, expressed similar strong objections for much the same reasons. The AFGE recognized with only limited satisfaction the inclusion in the Federal Personnel Manual of the partial bars to the use of polygraphs in screening applicants and appointees to competitive service positions, following subcommittee hearings of a decade ago. It expressed particular concern about that significant part of the Federal work force which is in the excepted service and which does not enjoy the same protection afforded competitive service employees.[22]

The AFGE proposed, therefore, that the use of polygraphs be controlled by legislation and that such legislation contain an absolute bar against the conduct of polygraph examinations of Federal employees, except in narrowly defined national security cases. The pressures placed upon certain elements of the intelligence and security apparatus of the Government were conceded to warrant the limited and selected use of polygraphs and other technological devices, in the public interest. However, it is the stated belief of the AFGE that the outer limits of that use and very strict procedural safeguards should be established under congressional standards, if proliferation of use and abuse in application is to be avoided.

The conditions which call forth the use of polygraphs on Federal employees are often highly charged investigations involving security breaches or leaks of classified information which initially at least are conducted under partial or total secrecy, according to the AFGE. In such circumstances, the compulsion upon the employee to consent is

[21] Hearings, pp. 38–49. See footnote 5 on p. 3.
[22] Hearings, pp. 384–385. See footnote 6 on p. 3.

believed to be almost overpowering. There is the assumption present—which the AFGE finds unwarranted—that the polygraph will somehow sort out the innocent from the guilty and that if an employee refuses to submit, he is hiding his guilt.

While the polygraph examination is not a surreptitious surveillance of the individual, like bugging or wiretapping or the use of two-way mirrors, the union believes that the use to which the results may be put can have the same deleterious effect, unless strictly controlled. Accordingly, assuming that polygraph examinations are warranted in narrowly justified circumstances, the AFGE proposed that they be conditioned unequivocally by law to require consent of the individual examined and to guarantee to him the right to have an attorney, a doctor, or both, or another representative of his choice present at all times during the examination.

The AFGE further proposed that absolutely no inference adverse to the employee should be drawn from the refusal to submit to the polygraph examination, that the use of the result of a polygraph examination be restricted to the specified purpose for which it was taken and to which the employee has consented, and that the use or distribution of such test results for any other purpose be prohibited.

The "Right To Prove One's Innocence"

Supporters of the use of the polygraph, psychological stress evaluator, and voice analyzer as "lie-detectors," who appeared before the subcommittee as witnesses, uniformly represented that their examination results were valid and reliable when their instruments were operated by competent examiners who adhered to proper examining techniques. They rejected the charge that use of these instruments violates an individual's constitutional rights and protections, supporting that view with the statement that the job applicant or employee has the option to refuse to take such an examination. Again, uniformly, they offered the view that the opportunity to take the polygraph or similar test should be welcomed by an individual, because, to quote the American Polygraph Association, "* * * all intelligent people endorse the right of the innocent to prove their innocence * * *."[28]

This latter view is a novel restatement of a major tenet of our system of jurisprudence that an individual is presumed to be innocent of charges brought against him and that his guilt must be proven.

A number of witnesses disagreed with this restatement of law. Mr. Henry S. Dogin, Deputy Assistant Attorney General, Criminal Division, Department of Justice, for example, was queried as follows:

> Mr. Cornish. One of the concerns that I raised here yesterday was sort of a theme running throughout the testimony of the polygraph proponents. And the theme was that there was a way a person can prove himself to be innocent of things. I just wondered, Mr. Dogin, do you know of any court in the United States where a defendant is required to prove his innocence?
>
> Mr. Dogin. No. The State, the people or the Government has to prove him guilty beyond a reasonable doubt.
>
> * * * * *

[28] Hearings, p. 191 See footnote 5 on p. 3.

Mr. Cornish. Also one of the witnesses yesterday said he thought it was a bizarre twist of the Constitution if someone were to regard the first amendment as giving the right to remain silent. Mr. Dogin, do you find that bizarre?

Mr. Dogin. Not at all.[24]

Proponents of the polygraph instrument stated during their testimony that, increasingly, courts have begun to admit test results as evidence. In response to the subcommittee's request, a summary of information bearing on that point was prepared and furnished by the American Polygraph Association (APA).[25]

Admissibility in Evidence

In substance, that submission discloses that a number of State courts have been considering more closely the subject of admissibility of polygraph test results as evidence. Examination by the subcommittee staff of the cases identified by the APA shows that the strongest of the cases have been in support of the defense; have dealt with situations where test results, although admitted through stipulation by both parties, were not admitted as prime evidentiary material; and none of the cited cases appears to have addressed those primary issues involving the violation of individuals' constitutional guarantees against self-incrimination.

Justice Department Position on Admissibility

The responsibility of the Criminal Division at the Department of Justice is to enforce all Federal criminal laws except those specifically assigned to that Department's Antitrust, Civil Rights, and Tax Divisions. U.S. attorneys are concerned with criminal matters and litigation arising under approximately 900 Federal statutes, including statutes relating to bank robbers, kidnapping, extortion, labor racketeering, fraud against the Government, conflict of interest, bribery of public officials, perjury, corruption of justice, and theft and larceny of public property. In light of these major responsibilities, the position of the Justice Department with respect to the use of results of polygraph examinations is deemed particularly noteworthy.

Because it views the results of those examinations with caution, it opposes their introduction into evidence at trial. To this end, U.S. attorneys are instructed not to seek the admission in evidence of polygraph examinations and to oppose all attempts by defense counsel to seek the admission of such examinations. This position of the Department of Justice is concurred in both by the eight U.S. courts of appeals which have considered the question of the advisability of polygraph results as evidence, and by the vast majority of State courts.

The Department of Justice witnesses, who appeared before this subcommittee, marshaled the following list of reasons supporting this policy:

First, while proponents of the polygraph claim 80 to 90 percent or even higher accuracy for the technique, their statistics are open to challenge because of the great difficulty in

[24] Hearings, pp. 631–632. See footnote 5 on p. 3.
[25] Hearings, pp. 147–153. See footnote 5 on p. 3.

obtaining independent corroboration of the results of the vast majority of examinations—especially those examinations indicating the subject was not trying to deceive the examiner.

Second, the results of polygraph examinations cannot be viewed with the same equanimity as the results of forensic tests such as fingerprints, ballistics, and blood tests because: (1) There is no specific physiological reaction indicative of deception, and even the same person may have inconsistent physiological reactions associated with deceptive responses; (2) apparent indications of deception may be caused by other psychological factors; (3) the moral attitude toward lying by the subject may affect his reactivity; (4) the subject may be able to "manufacture" physiological responses, such as intensifying his reactions to control questions, thereby effectively masking his reactions to relevant questions; (5) mental instability or aberration may affect the reactivity of a subject; (6) the taking of depressant drugs may affect a subject's reactivity; (7) the physical circumstances incident to an examination may affect a subject's physiological reactions; (8) the complexity and nature of the matters being inquired into may affect a subject's reactions (for example, a subject may be able to rationalize his answers in matters involving his state of mind, such as questions relating to intent or knowledge, but would be less likely to be able to rationalize his answers to simple direct questions such as "Did you shoot John Jones?"); and (9) other objective factors such as a subject's involvement in other similar acts, excessive interrogation prior to the polygraph examination, and excessive test length may also affect the accuracy of polygraph results.

In addition to these objective factors affecting the validity and reliability of polygraph results, subjective factors, such as the polygraph examiner's observation of the subject's behavior during the test procedure, the effect of the interaction of the polygraph examiner and the subject, and the subjective bias of the polygraph examiner, may all affect the validity and reliability of any examination.

Third, and possibly most important, because of the undue reliance juries are likely to place on the apparent mechanistic accuracy of polygraph results, we believe that the introduction in evidence of polygraph results would virtually vitiate juries' historical fact-finding responsibilities. As Judge Irving Kaufman eloquently stated fifteen years ago:

> The most important function served by a jury is in bringing its accumulated experience to bear upon witnesses testifying before it, in order to distinguish truth from falsity. Such a process is of enormous complexity, and involves an almost infinite number of variable factors. It is the basic premise of the jury system that twelve men and women can harmonize those variables and decide, with the aid of examina-

> tion and cross-examination, the truthfulness of a witness. * * * I am not prepared to rule that the jury system is outmoded. * * * I still prefer the collective judgment of twelve men and women who have sat through * * * a trial and heard all the evidence on the guilt or innocence of a defendant.

Indeed, unless there is a constitutional amendment which substitutes trial by polygraph for trial by jury, the Criminal Division will oppose the introduction in evidence of polygraph results.

Fourth, under the common law rules of evidence and proposed Rule 704 of the Rules of Evidence for United States Courts and Magistrates, polygraph results, which one Court of Appeals has perceptively referred to as little more than "electrical oath-helpers," would not be the proper subject of expert testimony.

Fifth, the admission of polygraph results would greatly attenuate the length of trials and lead to a potentially serious confusion of the issues. Our experience with hearings on defense attempts to introduce polygraph results in evidence is that these hearings take more of the courts' time than 75 percent of all criminal trials. It readily can be seen that such hearings not only would more than double the length of most trials, but also would lead to serious confusion of the issues involved in a case because at least as much of the court's time would be spent "trying" the polygraph examination as the issues involved in the case. Moreover, if courts admit polygraph results of defendants, should they not also admit polygraph results for key witnesses or even all witnesses?

Additionally, if the use of the polygraph becomes prevalent, jurors may come to believe that any defendant who does not submit polygraph results indicating his innocence is presumably guilty.

Sixth, it is our belief that there is no proper evidentiary purpose served by polygraph results which would justify their admissibility in evidence under either common law rules of evidence or the proposed Federal Rules of Evidence. Polygraph results are not properly classifiable as substantive evidence, evidence of character trait or credibility, or rehabilitative evidence as an exception to the prior consistent statement rule.

Finally, if the Government were to seek the introduction of polygraph results of defendants in cases in which defendants failed to testify, serious Fifth Amendment problems would arise. If defendants were to successfully introduce polygraph results in cases in which they did not intend to testify, serious questions would arise as to whether they did not thereby waive their Fifth Amendment rights and could be required to take the stand.[26]

---

[26] Hearings, pp. 413–417. See footnote 5 on p. 3.

V. POLICY AND STANDARDS ESTABLISHED BY THE CIVIL SERVICE COMMISSION

The current provisions of the Federal Personnel Manual relating to the use of polygraphs are an outgrowth of the interagency study made following the issuance by this committee of its reports in 1965 and 1966.

The first report recommended that the President establish an Interagency Committee To Study Problems Posed by the Federal Government's Use of Polygraphs and to work out solutions. The second report recommended that all Federal Government agencies be placed under a uniform administrative system which would enforce maximum controls on the use of polygraphs and would establish regulations to prevent their proliferation and misuse.

The study, under the direction of John W. Macy, Jr., then Chairman of the Civil Service Commission (CSC), developed a set of guidelines and instructions which, in substance, were incorporated by the Commission into a Federal Personnel Manual system letter issued October 25, 1968, and, subsequently, into the Federal Personnel Manual, chapter 736, appendix D.

Current Civil Service Commission Regulations

The current regulations, which include minor modifications made in 1973,[27] contain the following essential provisions:

> (1) An executive agency which has a highly sensitive intelligence or counterintelligence mission directly affecting the national security may use the polygraph for employment screening and personnel investigations of applicants for and appointees to competitive service positions only after receiving written approval from the Chairman of the Civil Service Commission.
>
> (2) The executive agency must submit to the Chairman of the Civil Service Commission a statement of the nature of its mission and a copy of its regulations and directives governing the use of the polygraph.
>
> (3) The Chairman determines whether the agency has an intelligence or counterintelligence mission directly affecting the national security and whether the regulations and directives meet the approval requirements.

Approval to use the polygraph is granted only for 1 year, and an agency given approval by the CSC to use the polygraph for competitive service positions is required to recertify annually that the conditions which led to the original certification still exist in the agency.

---

[27] Inst. 196, dated July 9, 1973, to Federal Personnel Manual, retained in subcommittee files.

All other uses of a polygraph to screen applicants for and appointees to competitive service positions are forbidden. This prohibition applies to the use of the results of polygraph examinations given previously by that agency, by another Federal agency, or by a private source.

The head of each department and agency of the Federal Government is responsible for establishing and maintaining an effective program to insure that the employment and retention in employment of any civilian officer or employee is clearly consistent with the interests of national security. The employment of each such civilian officer or employee is subject to investigation. The investigation of persons entering or employed in the competitive service is primarily the responsibility of the Civil Service Commission. Exceptions to that rule may be made where agency heads assume that responsibility pursuant to law or by agreement with the Commission. The investigation of persons other than those in the competitive service is primarily the responsibility of the employing department or agency.

Of the 2.6 million Federal civilian employees, 85 to 90 percent are estimated by the Civil Service Commission to be competitive service employees. The remaining 10 to 15 percent—or between 250,000 to 375,000 individuals—are excepted service employees. The use of polygraphs in personnel investigations of such excepted service employees, either for pre-employment screening or as a condition of continued employment, is not prohibited by the provisions of the Federal Personnel Manual.

Included in the category of excepted service employment are employees of the Tennessee Valley Authority, the employees of the Foreign Service in the Department of State, all—some 10,000—attorneys in the Federal Government (schedule A); cooks, chaplains and other persons for whom the Commission lacks either the capacity or opportunity to examine as to qualifications (schedule B); and those noncareer executive assignments frequently referred to as "political jobs" (schedule C).

The Civil Service Commission itself does not possess any devices such as the polygraph or a psychological stress evaluator, nor does it make use of those so-called lie detectors in its own internal operations or in discharging its responsibilities relating to Government-wide investigative activities. Its Bureau of Personnel Investigations, through the Office of Security Appraisal, conducts continuing studies of personnel security programs of Federal departments and agencies for the purpose of determining:

(1) Deficiencies in security programs established under the order which are inconsistent with the interests of, or directly or indirectly weaken, the national security.

(2) Tendencies in these programs to deny to individual employees fair, impartial, and equitable treatment at the hands of the Government, or rights under the Constitution and laws of the United States or Executive Order 10450.

Each study made at a department or agency includes examination of pertinent files and regulations, and looks into whether it is used only for approved purposes. An agency is required to take necessary steps to correct any material weakness or deficiency disclosed during the appraisal and to notify the Commission of the changes made. This

requirement would be applied to any unapproved use of the polygraph, or any similar device.

Commission's Assessment of Agency Polygraph Use

The Commission's experience, since the issuance of its instructions in 1968, leads it to conclude that little use has been made of the polygraph, in relation to competitive civil service employment. Only one agency, the Department of Defense, has submitted a request for approval of the use of the polygraph. The initial request dated June 20, 1969, was not approved by the Commission. By letter of July 8, 1969, Commission Chairman Hampton advised the Department of Defense that DOD Directive 5210.48, issued July 13, 1965, which governed the use of the polygraph throughout that department, needed to be updated and clarified so that it more specifically met the criteria set forth in the Federal Personnel Manual.

A second Department of Defense request, dated March 14, 1973, resulted in the Chairman of the Civil Service Commission granting authority to use polygraph examinations for certain limited categories of employees.[28] A request for renewal of this approval was under consideration by the Commission at the time of the subcommittee's hearings in June 1974.

The Civil Service Commission advised the subcommittee in March 1975 [29] that the Department of Defense had submitted its proposed regulations and directives on the use of polygraphs for review during the fall of 1974. The Commission returned that submission to the DOD, with suggestions for changes. During October 1974 DOD agreed to make the suggested changes and to have the revised guidelines approved by the Secretary of Defense. The Commission also advised that it was its understanding that after the guidelines had been approved and signed by the Secretary of Defense, DOD would apply to the Commission for permission to use the polygraph for a 1-year period under the amended guidelines. However, as of this latest advice from the Commission, the guidelines have yet to be signed and approved by the Secretary of Defense.

Security appraisals performed by the Civil Service Commission have disclosed no misuse of the polygraph by agencies. Its recent appraisal at the National Aeronautics and Space Administration (NASA) did disclose, however, that that agency had regulations setting forth a policy regarding polygraph examinations which did not conform to the provisions of the Federal Personnel Manual. The Commission's security appraisal of that agency was closed out on May 17, 1974, at which time NASA agreed to revoke its policy.[30] The Commission also was assured by NASA that the policy had not been used in violation of the provisions of the Federal Personnel Manual.

The committee notes with satisfaction that the Federal Personnel Manual now includes a statement of Government-wide policy with respect to the use of polygraphs by Federal agencies, where none existed at the time of its earlier hearings, 10 years ago. Additional evidence of concern by the executive branch is the continuing review by the

[28] Hearings, p. 412. See footnote 5 on p. 3.
[29] Letter retained in subcommittee's files.
[30] Hearings, p. 412. See footnote 5 on p. 3.

Civil Service Commission of agencies' security programs, including consideration of their policies and practices concerning the use of polygraphs.

The committee is convinced, notwithstanding, that additional opportunity exists throughout the Federal Government to improve and strengthen both policy and practices. The Federal Personnel Manual appears to be overly concerned with what agencies must do to obtain approval from the Civil Service Commission to administer polygraph examinations to their employees. It is the committee's belief that, in an area of such sensitivity with respect to individuals' rights, the pertinent paragraphs of its manual should state clearly those few specific conditions in which applicants for and appointees to competitive service positions may be required to take polygraph examinations. It also should state what effect the polygraph examination, or the refusal to take that examination, has on eligibility for employment or continued employment. Such an introduction would more appropriately preface the current explanatory material in appendix D of chapter 736 of the Federal Personnel Manual.

The testimony by the Civil Service Commission witness disclosed that only the Department of Defense has submitted a request for approval of its statement of policy and procedures applicable to use of polygraph tests to examine a few Defense Intelligence Agency employees in competitive service positions who were detailed to work with the National Security Agency. The subcommittee, by circularizing a questionnaire among 53 Federal agencies, learned that not only the Department of Defense but other agencies, including some with employees in competitive service positions, administered or had administered for them a number of polygraph tests during 1973.

The Department of Justice letter of November 26, 1973,[31] reports that its Drug Enforcement Administration utilizes the polygraph to evaluate employee integrity, when allegations concerning the employee are made, or to judge the credibility of informants who volunteer unusual information of an important nature. That letter further states that the Drug Enforcement Administration contracts with members of the American Polygraph Association for polygraph examinations, but that no costs were incurred for this purpose in fiscal year 1973.

The Board of Governors of the Federal Reserve System responded on November 12, 1973,[32] stating that on four specific occasions in fiscal year 1973 polygraphs were utilized, through the retention of outside agencies, as aids in the investigations of suspected improper conduct of duties by Reserve bank employees.

The November 14, 1973,[33] response from the United States Postal Service reports that polygraph examinations are used in criminal investigations of employees' activities and that 485 polygraph examinations were made by the Postal Service during fiscal year 1973.

The Defense Communications Agency responded to the questionnaire on November 2, 1973,[34] stating that it did not possess any polygraph machines, but that at the request of the Office of the Special Assistant

[31] Letter retained in subcommittee files.
[32] Letter retained in subcommittee files.
[33] Letter retained in subcommittee files.
[34] Letter retained in subcommittee files.

to the Secretary of Defense, it had arranged for the U.S. Army 902d Military Intelligence Group to conduct one polygraph examination during fiscal year 1973.

None of the above agencies included in their responses to the questionnaire any disclaimer that the tests were given to individuals other than employees in the competitive service category. The committee was unable to ascertain from the limited information furnished whether or not the polygraph tests reported to it by these four agencies were given to competitive service personnel. Information subsequently obtained confirmed that those provisions of the Federal Personnel Manual relating to the use of polygraphs are applicable neither to the employees of the Federal Reserve System nor the Postal Service, because those employees do not hold competitive service positions.

No procedure currently exists imposing the requirement that all agencies which have any competitive service employees and which do administer polygraph examinations report to a control agency in the executive branch, certifying that polygraph tests were not administered in connection either with pre-employment, appointment, or continuance of employment of such individuals. The committee is persuaded that, absent such a reporting requirement, the Civil Service Commission can only assume that no agency other than the Department of Defense is giving polygraph tests or has had polygraph tests given to its competitive service employees.

The committee is further persuaded that such periodic reporting is desirable at intervals not less frequent than annually. Such reporting should provide for the disclosure of the volume of polygraph testing, Government-wide, for both those agencies having highly sensitive intelligence or counterintelligence missions directly affecting the national security and for those agencies not members of that intelligence community. Those reports should cite the Civil Service Commission document containing approval of the agency's pertinent regulations and directives and should furnish data on the number of polygraph instruments; the number of tests administered both by and for the agency, categorized by purpose of the test (as contemplated by paragraph D–3(1) of appendix D); and the numbers of excepted employees and competitive service employees tested.

VI. OWNERSHIP AND USE OF "LIE DETECTORS" BY FEDERAL AGENCIES

Only a relatively few agencies in the Federal Government currently own and use polygraphs, and that same condition pertained when the committee made its report in 1965. The overall pattern of ownership and usage has changed only slightly in the intervening decade. Generally, polygraphs are being used in screening applicants for employment by the Central Intelligence Agency (CIA) and the National Security Agency (NSA); by these and several other agencies, in connection with security and personnel investigations of employees; and by two agencies in connection with scientific research not related to the subject of lie-detection.

Financial and Statistical Data

In 1965, agencies reported to the subcommittee ownership of 512 polygraphs which were acquired at a cost of $428,066, and which were used for 19,796 tests during fiscal year 1963. The subcommittee's recent canvass of agencies showed a reported ownership of 458 polygraph devices with an acquisition cost of $493,368, and that 6,889 tests were performed during fiscal year 1973. This decline in the volume of tests performed is particularly noteworthy, because the 19,796 tests given 10 years ago do not include those tests given by both the CIA and NSA, whereas the 6,889 total currently reported does include more than 3,000 tests performed by NSA. It is quite obvious that those other agencies (primarily the military departments in the Department of Defense) which own polygraphs also have sharply curtailed their use.

Some of the more significant data furnished to the subcommittee relating to the number and cost of polygraphs owned, and the frequency with which they were used during fiscal year 1973, follow:

USE OF POLYGRAPHS BY AGENCIES OF THE UNITED STATES GOVERNMENT

	Instruments owned	Acquisition cost	Annual maintenance and other expenses [1]	Tests performed in fiscal year 1973
Investigation and personnel screening:				
Department of Defense:				
Army	285	$219,171	$59,289	2,028
Navy	21	30,500	26,181	665
Marines	12	24,000	500	62
Air Force	58	53,872	47,410	482
Defense Investigative Service	0	0	0	5
Defense Communications Agency	0	0	0	1
National Security Agency	14	24,645	11,866	3,081
Defense Intelligence Agency	0	0	0	21
Chairman, Joint Chiefs of Staff	0	0	0	0
Defense Telephone Service	0	0	0	0
Total, Defense	390	350,189	145,246	6,325

See footnotes at end of table.

79-064 O - 76 - 12

26

USE OF POLYGRAPHS BY AGENCIES OF THE UNITED STATES GOVERNMENT—Continued

	Instruments owned	Acquisition cost	Annual maintenance and other expenses [1]	Tests performed in fiscal year 1973
Investigation and personnel screening—Continued				
Department of Justice: Federal Bureau of Investigation	26	$25,847	$500	79
Department of the Treasury:				
Secret Service	10	13,215	0	[2] 50
Customs Service	1	1,368	200	7
Total, Treasury	11	14,583	200	57
U.S. Postal Service: Postal Inspection Service	10	14,813	23,028	485
Central Intelligence Agency	[4]	[4]	[4]	[4]
Total, investigation and personnel screening	437	405,432	168,974	6,946
Scientific and medical research:				
Health, Education, and Welfare	19	74,990	0	0
Environmental Protection Agency	2	12,948	0	0
Total, scientific and medical research	21	87,938		
Total, all applications	458	493,370	168,974	6,946

[1] Exclusive of operators' salary costs.
[2] Tests administered in connection with, respectively, personnel security, personnel screening, and security clearance.
[3] Response stated: "Less than 50 polygraph tests were conducted by the Secret Service in fiscal 1973."
[4] Agency states such information is classified and its disclosure restricted under 50 U.S.C. 403(g).

The committee cautions that the data furnished by the Federal agencies reporting ownership and use of polygraphs have not been validated by audit or any other means, and that some evidence is at hand which raises questions about the accuracy of some of that reported data. The single largest user listed above is the Department of Defense, which furnished statistical data, first during November 1973, and subsequently during the public hearings in June 1974. There were some sharp disparities in those data, particularly as they related to the total number of polygraphs owned and in use by the Army and in the number of polygraph examiners in the various components of the Department of Defense.

The data reported on those two occasions are shown below:

DEPARTMENT OF DEFENSE COMPILATIONS OF DATA RELATING TO POLYGRAPHS AND POLYGRAPH EXAMINERS

	Polygraphs owned			Polygraph examiners	
	Operable	Inoperable	Total	Certified	Primary duty
Army:					
June 30, 1973	141	[1] 144	285	70	9
Mar. 31, 1974	276	140	416	61	32
Navy:					
June 30, 1973	21	----	21	10	10
Mar. 31, 1974	21	----	21	9	9
Marine Corps:					
June 30, 1973	12	----	12	11	0
Mar. 31, 1974	12	----	12	17	0
Air Force:					
June 30, 1973	58	----	58	33	0
Mar. 31, 1974	58	----	58	27	1
NSA:					
June 30, 1973	14	----	14	12	7
Mar. 31, 1974	16	----	16	20	7
Total:					
June 30, 1973	246	144	390	136	26
Mar. 31, 1974	383	140	523	134	49

[1] Shown as inoperable, on basis of DOD statement that many of the 144 units in the Army Materiel Command stock are obsolete.

The Department of Defense, at the request of the subcommittee, has undertaken to resolve those differences. That Department has furnished responses to the subcommittee's inquiries concerning (1) the need for the relatively large number of polygraphs (58) owned by the Air Force, in view of the relatively few tests (482) given by that DOD component in fiscal year 1973, and (2) the need for so many certified examiners in the Air Force, with all the attendant costs for qualifying them, inasmuch as only one person had that function as a primary duty.

On the first point, the Department of Defense stated that the Air Force's initial acquisition of the instruments was based on their distribution to each regional operating location, so that examiners did not have to carry an instrument with them at all times. In 1970, the Air Force changed its system to require individuals to carry their own individually assigned instruments. Excess instruments were maintained as backups for repair parts for the ones in use in the field. Plans to eliminate excess instruments in the Air Force inventory were being put into effect.

On the second point, the subcommittee was advised that, up until July 12, 1974, the Air Force had assigned polygraph duties as an additional duty, believing that this policy permitted timely administration of examinations. Due to programed revisions in the DOD Directive, the Air Force was planning to go strictly to primary duty polygraph examiners and would assign individuals with primary duties in that field.

This change was expected to result in a future cut of over 50 percent of the presently certified polygraph examiners in the Air Force's Office of Special Investigations (OSI), as well as a 50- to 75-percent cut in equipment requirements. The subcommittee subsequently was advised that the number of OSI polygraph examiners is being reduced from 34 to 17. DOD sources have estimated that, at the $20,000 average annual payroll cost for such individuals, total annual savings of a recurring nature would approximate one-third of a million dollars. This would be reduced, in some small measure, by increased travel costs incurred by the remaining examiners.

Significant additional savings are anticipated by the Department of Defense as a result of reductions in future years' requirements for training of examiners and for procurement of polygraph equipment.

Use of Psychological Stress Evaluator

The psychological stress evaluator (PSE), marketed by Dektor Counterintelligence & Security, Inc., is a comparatively new entry in the field of lie detector devices. Relatively few have been acquired by Federal agencies, with the Department of Defense being the principal purchaser. The following data on sales to Federal agencies were furnished by Dektor.[35]

[35] Letter retained in subcommittee files.

28

Agency	Date of sale	Number of items	Serial No.	Number of operators trained
NASA Ames Research Center, Moffett Field, Calif.	June 22, 1974	1	1560	2
Patuxent Air Test Center, Patuxent, Md.	May 24, 1974	1	1572	2
Human Engineering Labs, Aberdeen Proving Grounds, Aberdeen, Md.	Nov. 14, 1973	1	1493	1
Sharpe Army Depot,* Lathrop, Calif.	July 1973	1	326	*2
VA Hospital, Danville, Ill.	Apr. 19, 1973	1	233	1
Drug Rehabilitation Center,* U.S. Naval Air Station, Yukon, Fla.	July 5, 1972	1	63	*2
United States Air Force, Office of Special Investigations,* Washington, D.C.	May 1972	1	51	*1
United States Army Mobility Equipment Research and Development Center, Combat Development Command, Fort Belvoir, Va.	Jan. 24, 1972	2	31, 32	1
Fort George G. Meade, Fort Meade, Md.	May 1972	1	10	0
Aberdeen Proving Ground, Aberdeen, Md.	do	1	6	0
Total		11		12

*Dektor also advised that the individuals it trained as PSE operators for the agencies marked (*) on the above list asked that the purchases by their sponsoring agencies be kept confidential.

When the agencies responded to questionnaires released at the subcommittee's request, their information was somewhat at variance with the above. The Veterans' Administration confirmed the acquisition of one PSE unit which was being used at a VA hospital in the treatment of psychiatric patients. An initial response from the Department of Defense reported the purchase of six PSE units through fiscal year 1973 by major DOD components. However, an amended DOD submission on May 9, 1974, reported that those components owned only five PSE's and that a voice stress analyzer purchased by one of its components, the National Security Agency, had previously been reported erroneously as a PSE. These five PSE's were procured at an average cost of $2,150 each for the purpose of determining their validity and possible usefulness.

The Department of the Army, which purchased three of the devices, contracted for a test and evaluation project by Fordham University at a cost of $27,492. The Fordham tests, summarized in an August 1973 report, found that the PSE produced valid results in less than one-third of the tests administered and that its reliability was less than pure chance. As a result, the Army dismantled two of the equipments and transferred the other to the Air Force for tests in an application not related to "lie detecting," personnel security, or investigations.

The Air Force Office of Special Investigations procured one PSE (in addition to that mentioned above obtained from the Army) for validation testing. The Air Force evaluation, encompassing approximately 60 tests during fiscal year 1973, although tentative, resulted in a conclusion that the device was not useful. This device was to be transferred to a Research and Development Office of the Air Force Research Laboratory, at Hanscom Field, Mass.

The National Security Agency obtained one PSE and also a voice stress analyzer for research purposes. Both devices were found to be insufficiently reliable. Both were declared surplus and made available for other research use unrelated to detection of deception.

Some discrepancies still remain between the number of PSE's reported as purchased by DOD, and the number reported by Dektor

as having been sold to DOD. Moreover, preliminary discussions with DOD personnel indicate that the purchases of at least two additional PSE instruments in fiscal year 1974 did not conform to prescribed procurement procedures. The subcommittee is also seeking some explanation from DOD why, on the one hand, PSE's are being dismantled and disposed of by one of its components because of their lack of reliability, and, on the other hand, subordinate organizations in the military components continue to contract for and acquire the same type of instruments.

Use of Voice Analyzers

In addition to the voice stress analyzer purchased by the National Security Agency, the subcommittee was advised that a Mark II voice analyzer, a conceptually different equipment item marketed by Technical Development, Inc., was purchased by the Central Intelligence Agency in May 1974, at a cost of $3,500. The CIA is evaluating that device, prior to making a firm decision as to whether to engage in any serious research.

Intelligence Agency Practices Differ

A number of Federal agencies having highly classified security missions require their civilian employees to be polygraphed as a part of the pre-employment screening process.

The CIA routinely uses the polygraph as an aid to investigation for determining the security eligibility of persons for employment by or assignment to the Agency; security clearance by the Agency; staff-like access to sensitive Agency installations; utilization in operational situations; or continued access to certain classified information. All CIA employees, except the Director and Deputy Director who are Presidential appointees, are required to take polygraph tests prior to appointment.

The National Security Agency (NSA), which is a separately organized agency within the Department of Defense, performs highly specialized technical functions in support of intelligence activities of the United States as one of its two primary missions. NSA's policy [36] is to use the polygraph examination as an investigative aid in determining the eligibility of persons for employment, and/or for access to sensitive cryptologic information or for access to certain areas. It also uses the polygraph in the conduct of counterintelligence and personnel security investigations which cannot be completed through normal investigative means.

All civilian employees of the National Security Agency, including Presidential appointees, are required by that Agency's regulations to be polygraphed as part of the pre-employment screening process. As a general rule, NSA's military personnel whose clearances are controlled by their parent service are not polygraphed.

---

[36] National Security Agency Regulation 122–3, dated Jan. 7, 1966, retained in subcommittee files.

The President's Foreign Intelligence Advisory Board, consisting of 12 individuals, advises the President concerning the various activities making up the overall national intelligence effort. It conducts a continuing review and assessment of foreign intelligence and related activities in which the Central Intelligence Agency and other Government departments and agencies are engaged and reports its findings, appraisals and recommendations to the President. The Executive order [37] establishing the Board provides that:

> The Director of Central Intelligence and the heads of all other departments and agencies shall make available to the Board all information with respect to foreign intelligence and related matters which the Board may require for the purpose of carrying out its responsibilities to the President.

When queried by the subcommittee,[38] the Board stated that neither appointment as a member of the Board, nor as the Board's Executive Secretary, nor as an employee on the Executive Secretary's staff was contingent on taking and passing a polygraph test.[39]

The State Department, the Federal Bureau of Investigation in the Department of Justice, and several major components of the Department of Defense have a considerable degree of involvement with the intelligence communities and deal in highly classified and very sensitive material, much of it relating to national security matters. These agencies see no need for routinely polygraphing their employees in connection with pre-employment screening interviews, and do not require such testing.

Testimony by the Department of Defense witness included the statement that in October 1972, the Department barred the use of the polygraph as a screening or selection device or as a condition of employment for all civilian employees—competitive service or excepted service—aside from those few individuals assigned to the National Security Agency. More recently, the Department advises that a proposed revision to its DOD Directive 5210.48 dealing with polygraph examination, when approved and issued, will make its provisions applicable to military personnel as well as civilian employees. This is another commendable action on the part of the Department of Defense, which earlier was commended for having taken the first step by any Federal agency to curtail the then-existing widespread use of these so-called lie detectors.

Does the Intelligence Community Rely Too Heavily on Polygraph Testing?

Dr. Stefan T. Possony of Stanford University's Hoover Institution on War, Revolution and Peace, who was not able to appear personally before the committee as a witness, did furnish a statement. In it he recognized the potential of the polygraph as a pioneering technological development which could contribute to achieving a better understanding of the interrelationships between psychological states and

[37] Executive Order 11460, dated Mar. 20, 1969.
[38] Appendix B.
[39] Appendix C.

physiological. However, he criticized in strong terms the present uses of polygraphs as "lie detectors," particularly in the intelligence and military communities, which are the principal users in the Federal Government.

The opening paragraphs of Dr. Possony's statement [40] include the following:

> I am not opposed, on principle, to the use of the polygraph in security investigations. I have no quarrel with the contention that from time to time, the polygraph has helped to uncover information which but for the use of the instrument might have remained hidden. But it is imperative that the polygraph be used in a manner that is scientifically and legally appropriate.
>
> I am not opposed to, or even particularly critical of, the system through which the United States Government seeks to prevent infiltration by hostile agents and, more generally, to protect its internal security. American investigators and security agencies have a difficult and thankless job to perform, and their freedom of action has been unduly narrowed by legal and political constraints. They do need all the technical support they can get, and it is not surprising that they are infatuated with a gadget which promises easy answers.
>
> I should add that the American internal security set-up differs most significantly from the despotic and inhumane police systems of the totalitarian states. But it does not live up to the standards this nation has chosen to observe and represent.
>
> * * * * *
>
> It is surprising, and disturbing, that the government has never yet taken a firm stand against the "lie detection" hocus-pocus. Like any technology which we incorporate in airplanes, ships or tanks, or any medical technique which we allow our physicians to use, or any drug which is released to the drugstore, the polygraph must be approached on the basis of scientific objectivity, technical excellence, statistical validation, investigative probity, administrative integrity, and legal acceptability.

The inadequacies and shortcomings of the polygraph examination in meeting reasonable criteria in each of the above areas are discussed in some detail in Dr. Possony's statement. In his judgment, the polygraph has been oversold as an instrument of personnel selection and counterespionage as well as an instrument of intelligence collection. It has also been oversold as the key to psychodiagnostics. In concluding his statement, Dr. Possony expressed himself as follows:

> To be viable, internal security programs must be kept within the confines delineated by the U.S. Constitution, including the Bill of Rights.
>
> If and when these basic points are finally grasped—but not before—psychodiagnostic research may begin to turn from fake to fact.

---

[40] Hearings, pp. 667–774. See footnote 5 on p. 3.

VII. POLYGRAPH OPERATORS AND THE QUEST FOR PROFESSIONALISM

The operator of the polygraph is generally conceded to be the most important component of the "lie detection" technique. He should have proper training and adequate experience to understand the theory on which the polygraph instrument is based, and should be aware of the device's limitations. Because of this, polygraph operators should be individuals of high moral character and sound emotional temperament, be selected carefully, trained properly, and supervised effectively.

On the basis of agency-furnished information showing variances among agencies on the points of minimum age, educational requirements, grade or rank, and investigative experience, the committee concluded in its prior report:

> * * * there are no uniform criteria for selecting Government polygraph operators, and training procedures are even more inconsistent. Both are completely inadequate since the operator is by far the most important factor in the polygraph technique.[41]

The consensus of witnesses at that time was that ideal minimum requirements for a polygraph examiner should include:

1. At least 25 years of age.
2. College graduate from an accredited school.
3. At least 5 years of investigative experience.
4. A complete background investigation, satisfactory completion of psychological tests, and a psychiatric review.
5. High moral character and sound emotional temperament.

Current Criteria for Selection of Examiners

Provisions of the Civil Service Commission's Federal Personnel Manual (FPM) pertinent to the use of polygraphs currently do include a requirement that agencies subject to the provisions of the FPM establish adequate standards for the selection and training of examiners, but do not prescribe such standards. Accordingly, an agency using polygraphs may, and still does, establish its own standards for qualifying individuals as polygraph examiners. It should come as no surprise that substantial differences still exist in the specific criteria that agencies have imposed upon themselves.

There is general acceptance by the components of the Department of Defense of the 25-year minimum age as one criterion as well as a requirement that the examiner be a citizen. Another agency gives its age criterion as a preference for "maturity consistent with about 30 years of age"; still another states that examiners should be between 25 and

[41] H. Rept. 89–198, p. 15.

40 years of age. In neither of these latter two instances is citizenship a stated requirement. The criteria for polygraph examiners furnished by two additional agencies are silent on the points of both minimum age or citizenship.

Various combinations of formal education and experience—involving type, level, and duration—are acceptable to different agencies to meet their minimum requirements for selection as polygraph examiners. Some agencies are silent in their statement of requirements on whether and how an individual will be judged as having high moral character and sound emotional temperament. At least one prescribes that polygraph examiner-designees themselves be subjected to a polygraph examination and a psychological assessment. Minimum grades and rank held by polygraph examiners still differ among the agencies.

From the foregoing, it is apparent that the standards for selection of individuals to be trained as polygraph examiners still are not uniform. However, the committee does discern some little movement by Federal agencies in that direction, and commends such efforts.

Polygraph Examiner Training

A substantial number of the polygraph examiners employed by Federal agencies have been trained at the Army's special training facility at the U.S. Army Military Police School, Fort Gordon, Ga. That training program, which was established in July 1951, originally was 8 weeks in duration; however, in July 1965, the course was extended to 12 weeks and then in August 1970, lengthened to 14 weeks. In addition to the 14-week formal training phase, each examiner-trainee must serve an internship prior to certification as a polygraph examiner.

The facility at Fort Gordon trains polygraph examiners not only for the Army, but also for the Air Force, Navy, and Marines, and for the Department of the Treasury and the U.S. Postal Service. The Army has also trained polygraph examiners for the U.S. Coast Guard; the National Security Agency; U.S. civilian police agencies under the sponsorship of the Law Enforcement Assistance Administration; Canadian Defense Forces; Philippine Army; Republic of Korea Army; Pakistani Army; Republic of Nationalist China Army; and the Venezuelan Army.

Since this training program was established in 1951, there have been 1,251 individuals graduated from the basic course; advanced, refresher, or personnel security training has been given to 270 students.

Department of Defense training

The prerequisites for attendance at the Army school by all DOD personnel include—U.S. citizen, at least 25 years of age, baccalaureate degree from an accredited college, plus 2 years experience as an investigator with a recognized government agency; or the equivalent of 2 years of college, plus 5 years of investigative experience. Personnel attending the course from other Federal agencies must meet prerequisites as determined by their respective agencies.

There are 506 academic hours in the polygraph examiner (basic) course, which includes 13 hours of polygraph theory and administration, 19 hours of polygraph maintenance management, 84 hours of polygraph examination procedures, 34 hours of training regarding

evaluation of mental and physical fitness of examinee, 331 hours of comprehensive practical exercises, and 25 hours of examinations. There are also 54 hours of nonacademic (administrative) time included in this course, with a total course time of 560 hours or 14 weeks. Based on fiscal year 1974 funding, the cost per student for this basic course is approximately $6,300.

The polygraph examiner refresher course, a 3-week or 120-hour course, affords advanced or refresher training for the practicing polygraph examiner and the requalification and certifications of previously trained personnel who have not been active as polygraph examiners. This course provides refresher training in all facets of polygraph examination procedures and polygraph instrumentation, as well as subjects related to the conduct of polygraph examinations.

DOD encourages its polygraph examiners to receive advanced or refresher training each 2 years at either the U.S. Army Training Facility or at other training seminars or workshops.

The internship prior to certification within the military departments of DOD is 6 months to 1 year in length, following the formal phase of polygraph training. During this period, each examiner conducts polygraph examinations in support of criminal or security investigations wherein polygraph charts are generated. All examinations conducted by intern examiners are directly supervised by a certified examiner.

The Department of Defense witness referred specifically, in recent testimony, to the concern previously expressed about the qualifications of polygraph examiners of that agency. The committee's prior report recognized that the DOD Directive 5210.48 established relatively high qualifications but then noted that it contained a grandfather clause which permitted examiners on the rolls in 1965 to continue on their jobs even if they did not have the training and education required under the agency's revised 1965 standards. The witness stated that the problem appears to have been resolved by the passage of time, in that there was only one such polygraph examiner remaining on Defense rolls. Moreover, that one individual had received refresher training as recently as December 1973. The other 134 examiners reportedly met fully the qualification standards of the DOD directive.

Other agency training of examiners

Currently, the National Security Agency examiners receive their polygraph training at the Keeler Polygraph Institute in Chicago, Ill. Following this training of 6 weeks duration, National Security Agency examiners serve an internship of 6 months or conduct 100 polygraph examinations under the direct supervision of a certified National Security Agency examiner.

The Central Intelligence Agency, under its centrally controlled program, also trains its own polygraph examiners. The training courses average 6 to 7 weeks in duration and include coverage of interviewing and interrogation, test construction, chart interpretation, instrument maintenance and repair, physiology, psychology, and professional ethics. On completion of this course of instruction, the trainee serves an internship of from 6 to 8 months, during which he is assigned cases of gradually increasing complexity under the guidance and monitoring of senior examiners.

The Federal Bureau of Investigation, too, conducts its own training program for polygraph operators. Agents selected for that training are provided an intensive 2-week academic program, followed by a 1 year period of on-the-job training, during which all their polygraph examinations are under supervision of the FBI Laboratory. The FBI does not send any of its agents to outside agencies or schools, public or private, for polygraph training.

The scope of training offered by the U.S. Army's school at Fort Gordon appears to be substantially more comprehensive and presumably more costly than that adopted by these other agencies for their own use. If its length and content can be justified as being minimally essential, then the adequacy of the courses developed by the CIA and FBI, and possibly NSA, is brought into question. If the shorter term courses of these latter agencies are adequate, then the Army's course which is twice the length of any of the others, may be unjustifiably lengthy and costly. Certainly, on either the point of effectiveness or economy, the committee believes that this matter warrants attention.

Efforts Toward Professionalism

The American Polygraph Association was formed in August of 1966 by a merger of three predecessor organizations—the Academy for Scientific Interrogation, the American Academy of Polygraph Examiners, and the National Board of Polygraph Examiners.

The 376 members in good standing of these predecessor organizations were accepted as charter members of the new organization. Those individuals then actively serving as polygraph examiners who did not meet the normal membership requirements prescribed by the APA constitution were permitted full membership status, by a provision for waiver of certain requirements. That waiver procedure was in effect for approximately four years after the APA was established. Membership in the APA totaled 1,004 by May 1974, and of this number, 645 were full members with the right to vote.

The APA constitution contains the following statement of objectives:

> The objectives of the American Polygraph Association shall be to advance the use of the polygraph as a profession as a means of promoting social welfare by the encouragement of the use of the polygraph in its broadest and most liberal manner; by promotion of research into instrumentation and techniques; by the improvement of the qualifications of polygraph examiners through high standards of professional ethics, conduct, education and achievement; to unify polygraph examiners throughout the world and rekindle their interest in the use of the polygraph and in the APA, by the increase and diffusion of polygraph technology through meetings, professional contacts, reports, papers, discussions and publications; thereby to advance scientific, professional and public acceptance of the contributions of polygraph techniques to the promotion of the public welfare and to keep the APA informed of member sentiment and urge the member-

ship's active participation in civic and community affairs where the polygraph is concerned; and to publicize the name and prestige of the APA.[42]

In furtherance of those objectives, the APA has, among other things, developed for its membership a code of ethics, standards, and principles of practice; publishes a quarterly journal and monthly newsletter; and expends considerable effort supporting licensing or regulation of polygraph examiners by the individual States.

In conjunction with this latter activity, it has drafted a model licensing bill which would regulate persons who purport to be able to detect deception or to verify truth of statements through the use of instrumentation as lie detectors, polygraphs, deceptographs, and/or similar or related devices and instruments.

The APA's board of directors adopted a resolution in August 1973, disapproving the use of the Dektor psychological stress evaluator as the sole source of or a major contribution to a determination of truth or deception in a meaningful testing situation for determining either truth or deception.[43] It also authorized its officers, directors and members to state the following as the official position of the APA, with reference to the Dektor PSE–1 psychological stress evaluator:

1. That the PSE–1 is not a polygraph and does not meet minimum standards for polygraph instruments; neither does it meet minimum instrument standards for those States which have established such standards by legislation.

2. That the published standards for the selection and training of PSE–1 examiners do not in any way meet APA requirements.

3. That the published capability of the instrument for surreptitious use constitutes a potential violation of the constitutional rights of the person being examined.

4. That the PSE–1 should not be used in a meaningful testing situation without verification by a trained examiner using an acceptable polygraph instrument.

There are, according to APA's recent testimony, 17 States which either license or regulate the activities of polygraph examiners.[44] In the remaining 33 States, any individual who either owns or has access to a polygraph device may offer his services as a polygraph examiner, for a fee, without meeting any prescribed minimum requirements of education, training, experience, or moral, and financial responsibility. No States have yet enacted licensing or regulatory statutes for users of the PSE device, and only the State of Florida has held public hearings on the proposition.

The APA also has a program for accrediting schools which train polygraph examiners. Its most recent listing of such schools shows 10 in the United States, including the Army's Military Police School and Texas A. & M. College, College Station, Tex.; the Israeli Polygraph School in Tel Aviv, Israel; and 2 accreditation actions pending.

Efforts by polygraph examiners to obtain acceptance of their activities as a profession and of themselves as professionals are wholly

[42] Hearings, p. 192. See footnote 5 on p. 3.
[43] Hearings, pp. 218–219. See footnote 5 on p. 3.
[44] Hearings, p. 146. See footnote 5 on p. 3.

understandable. Raising the requirements for education, training, work experience and personal qualifications of those individuals whom the APA certifies as polygraph examiners is a goal that the committee finds laudable. The committee, however, retains much of its earlier reservation about whether the broadly stated APA requirement of a baccalaureate degree, irrespective of the discipline involved, is a reasonable criterion for properly qualifying an individual as a polygraph examiner. The committee would deem it more appropriate, absent special professional-level medical training of individuals, that polygraph examiners have at the very least a substantial educational background in psychology, physiology, and human behavior.

The relatively minor role accorded such subjects in those polygraph training course curriculums furnished to the subcommittee falls short of what it feels is acceptable preparation. The committee's position, in its 1965 report, was that qualified physicians and psychiatrists should be among the appropriate officials designated to review polygraph examination records. Little evidence was offered or representations made by agency spokesmen during the recent hearings that this recommendation has either been adopted or given serious consideration. The following commentary, offered by Dr. Possony, appears to have particular relevance:

> If we compare the polygraph with a medical specialty, we can say that the polygraph is a quasi-medical specialty which was taken over by the nurses. The doctors are not admitted to practice in this field, the scientific backup is woefully inadequate, and the current expectations on performance are too high. If the general philosophy which the U.S. Government is applying to public health were adhered to with respect to the polygraph, this machine would be restricted to specialists with high rather than low qualifications. Furthermore, the utilization of polygraphs in private industry would be forbidden.
>
> To find methods permitting the effective diagnosis of psychological and mental states has been one of the most challenging tasks throughout history. This task, which was not solved even by torture and which remains unsolved, is continuing but it cannot possibly be entrusted to individuals with perfunctory preparation. In the United States, to pull a tooth, one must have a dental degree. To handle a mild neurosis, one needs a degree in clinical psychology. To perform surgical operations, one must be a highly qualified and certified surgeon. Of course, medical doctors cannot function without nurses and nurses aides. Similarly, in the polygraph field, some tasks can be performed by the "operators". But it is entirely inappropriate to use such operators as diagnosticians and to allow them to work without professional supervision.[45]

[45] Hearings, pp. 710–712. See footnote 5 on p. 3.

VIII. THE POLYGRAPH TEST AND SAFEGUARDS FOR THE INDIVIDUAL

In one of its early studies[46] the Foreign Operations and Government Information Subcommittee cataloged the reasons given by Federal agencies for the use of polygraph examinations in carrying out Government business. These included the investigations of security matters, infractions of criminal laws, and employee misconduct, as well as pre-employment screening, medical measurements, and medical and scientific research. Regardless of the stated use, those agencies assured the subcommittee that the rights of individuals who were given polygraph tests were adequately safeguarded. Presumably those assurances relied heavily on the corollary representations that individuals voluntarily agreed to submit to such tests.

Another, clearly less defensible reason for using polygraphs recently was disclosed in the record of transcription of Presidential tapes released by the House Judiciary Committee in 1974. The following statement reportedly was made by President Nixon in an Oval Office conversation on July 24, 1971, because of his concern and frustration with repeated leaks to the press about his secret foreign policy positions:

> Listen, I don't know anything about polygraphs and I don't know how accurate they are but I know they'll scare the hell out of people.[47]

The President reportedly proposed giving lie detector tests to as many as 1,500 people with "top secret" security clearance in the National Security Council, State Department, Central Intelligence Agency, and the Department of Defense, but was persuaded by his aides not to do so, at least as an initial step.

As previously stated, the circumstances under which many polygraph tests are given are potentially if not actually coercive, from the individual's viewpoint. For that reason, the committee has had and continues to have considerable concern about the safeguards for the individuals. Accordingly, agencies were asked for information about the organizational level at which approval to give a polygraph test must be obtained, whether an individual's physical and mental condition are considered, whether the use of polygraphs is subject to review, what relative weight is accorded polygraph test results or refusals to be tested, whether test results are made known to the individual, whether an avenue of appeal exists, and what controls exist to insure the confidentiality of those test results.

---

[46] "Use of Polygraphs by the Federal Government (Preliminary Study)," committee print, April 1964, 88th Cong., 2d sess.
[47] Washington Post, July 10, 1974.

A number of these high-interest areas are matters that must be covered in the agency regulations and objectives that the Civil Service Commission requires to be submitted to it, when agencies elect to use the polygraph in personnel investigations of competitive service employees and applicants to competitive service positions. Examination of the regulations and directives and questioning of witnesses during the subcommittee's hearings disclosed a number of significant differences among agencies in their implementation actions.

Who Authorizes Tests?

In most instances, agencies now are requiring that polygraph tests not be given until written approval has been obtained from a relatively high level official authorizing the action. Only in a few instances are such approvals authorized at a field level, without requiring prior approval at the headquarters level in Washington.

The Director of the Central Intelligence Agency has delegated to his Director of Security authority to conduct the polygraph program for that Agency. The Director of the National Security Agency has delegated a general authority to that Agency's Director of Security to polygraph applicants for employment; employees of contractors requiring access to the Agency's spaces, classified information, or classified operations; and persons assigned to unusually sensitive projects. Specific written approval of the Director of Security or a higher authority is required in each case when polygraph examinations involving counterintelligence or personnel security investigations are proposed.

Requests for polygraph examinations in the Federal Bureau of Investigation are referred through channels to supervisory review levels at the agency's headquarters, and final approval authority is vested in Assistant Directors. The U.S. Postal Service, which uses polygraph examinations in those criminal cases which are under investigation by its Inspection Service, has established two levels at which approval may be authorized. The Regional Chief Postal Inspector has authority to authorize the use of the polygraph in the field; in certain exceptional cases, the Postal Service's Chief Postal Inspector may personally authorize use of the polygraph.

Two organizational elements in the Department of Treasury use polygraphs—the Customs Service and Secret Service. Both the Office of Investigation and Office of Security and Audit in the Customs Service must obtain prior approval from the Assistant Commissioner (Security and Audit). In the Secret Service, polygraph testing may be authorized by the Special Agent in Charge of a Field Office, or, on request of that Special Agent in Charge, the matter may be referred for approval by the Assistant Director at headquarters in Washington.

The State Department, although it does not own polygraph devices, reports that on rare occasions in the past it has used the polygraph examination as one of a number of investigative techniques to resolve discrepant testimony by employees suspected of activities prejudicial to national security interest. On such occasions, these services were obtained by contracting out. Final approval authorizing a polygraph

examination must be made by the Department's Deputy Assistant Secretary for Security, if a case supervisor responsible for a particular investigation recommends that course of action.

Consideration of Physical and Mental Condition

The polygraph is one of many instruments used for measuring the physiological changes that frequently accompany changes in an individual's feelings. Gaging an individual's physical or mental condition and determining whether or not that state of health is "normal," is, in the committee's opinion, a matter for medical professionals. That was one of the bases for its earlier recommendation that qualified physicians and psychiatrists should be included among the appropriate supervisory officials designated to review polygraph examination records.

Information furnished to the subcommittee shows that the Central Intelligence Agency, alone, among those agencies frequently using polygraphs, routinely requires that (a) examinees be interviewed by representatives of the Office of Personnel and the Office of Medical Services and (b) those Offices advise the Director of Security of anything known to them that might preclude the advisability of conducting a polygraph interview.

At the other end of the spectrum, the U.S. Postal Service appears to depend on the qualifications of its polygraph operators to make those medical-type determinations. That agency responded to the subcommittee's inquiry as follows:

> The physical and mental condition of the person to be tested is evaluated by the Postal Inspector who conducts the polygraph examination. Written instructions regarding such an evaluation are not made; however, evaluation of the subject's mental and physical condition as a prerequisite to the test is a part of the formal training each Polygraph Examiner receives in polygraph school. Questions regarding the physical and mental condition of each subject are asked by the Examiner before the examination is commenced, and a record is made of the responses to such questions.

The responses of other agencies fall somewhere between these extremes. Two agencies, stating that the physical and mental condition of the person to be tested is considered—"carefully considered" by the Department of Justice and "always considered" by the Department of State—did not disclose whether that consideration and conclusion was by polygraph operators or by qualified medical professionals. After further inquiries, these two agencies advised that an individual for whom a polygraph test is being contemplated may be referred to a medical professional for interview or examination, if a question or doubt about the individual's physical or mental state of health arises.

The Department of Justice requires that the request for approval of polygraph testing that is transmitted to Washington be accompanied by an identification of any known physical or mental disabilities, abstracted from the background file on the individual. On the basis of that data, the approving official may recommend that the

examinee be advised to consult with his personal physician before the test. The polygraph examining procedure used by its Federal Bureau of Investigation in the pretest interview also includes as a further measure of assurance inquiries by the polygraph examiner concerning the examinee's state of health.

The Department of State also considers any pertinent health and medical information available in the employee's personnel file, and solicits the views of the investigative case supervisor and the polygraph examiner in deciding whether an individual should be polygraphed or should be referred for a professional medical examination before being given the polygraph test.

In the case of the National Security Agency, if its polygraph operators have any question or doubt as to the physical or mental fitness of any examinee, they may refer the matter to the Director of the Medical Center for appropriate action. From the information provided to the subcommittee by the Department of the Treasury, it appears that investigative personnel in its Bureau of Customs and Secret Service make the determination of condition of health without any prior advice or consultation with medical personnel.

Weight Accorded Polygraph Tests

The stated policies of agencies using polygraphs appear relatively consistent on this point. In substance it is best exemplified by the Departments of Justice and State, where the polygraph examination is held to be a useful adjunct to the normal interview and interrogation process, and may provide direction for additional investigative effort. Information developed during such examinations reportedly is given the same weight as substantive information developed from any other source.

The CIA and NSA both require applicants for employment to be polygraphed, as one aspect of their security screening processes. Both agencies represented to the subcommittee that, while refusal to take a polygraph test would effectively bar an individual from further consideration for employment, the result of the test is but one element of the total investigative record and that security action is not taken on the basis of the polygraph test results alone.

The U.S. Postal Service uses polygraph tests most frequently where large numbers of persons have had access to registered mail which has been lost, and an effort is being made to narrow the number of suspects. The use of the polygraph in such circumstances is justified by the Postal Service as an expedient means of saving many investigative hours and of providing definite suspects on whom the investigative energy can be concentrated.

In the Treasury Department, the two organizations which use polygraphs state their policy somewhat differently. The Secret Service claims to use polygraph tests only after other factors have been determined which indicate that this technique may be of further assistance. It is not considered to be anything other than an aid in a criminal investigation. It is not used as a substitute for personnel investigation or interrogation of a suspected person.

79-064 O - 76 - 13

The Customs Service advised the subcommittee that the polygraph is used only when tangible and concrete investigative leads have been exhausted, but also stated that the results of such examinations are used as investigative aids rather than as evidence. Most commonly these tests are used to determine an individual's involvement or non-involvement in cargo theft cases or cases of personnel dereliction areas. In a number of cases, polygraph examination results are credited with having determined involvement and complete confessions and the identification of coconspirators followed.

Effect of Refusals To Be Polygraphed

Agencies responding to the subcommittee's current inquiry were consistent on several pertinent points. Polygraphs are given only with the voluntary consent of the individual to be tested. Refusal of an individual to agree to take a polygraph test is not recorded or reflected in that individual's official personnel file.

A fairly representative statement on this point is the instruction of the U.S. Postal Service, which reads as follows:

> REFUSAL TO TAKE AN EXAMINATION
>
> 44.17 The polygraph examination is voluntary in nature and no person can be forced to take an examination. The examination requires the full and complete cooperation of the Examinee. A Postal employee who declines to take an examination shall not be considered as failing to cooperate in an investigation. No stigma is attached to such a refusal, and adverse action shall not be taken against a person for unwillingness to volunteer to take a polygraph examination. Information concerning a person's refusal to submit to a polygraph examination shall not be recorded in any of his personnel files.[48]

The very nature of the polygraph equipment and the examining procedures used in a test is such as to preclude giving the test unless the individual's "cooperation" is obtained. Whether or not such cooperation is indeed evidence of "voluntary" consent has been noted previously in this report. The inherently coercive pressures to submit to an examination, both for those who are asked to do so in connection with employment screening programs of the CIA and NSA, or for those other Federal employees who may believe that continuance in their positions would somehow be compromised if they did not submit, are relatively self-evident.

The CIA witness offered the following commentary on that Agency's cyclical reinvestigation program, in connection with which employees may be asked to take another polygraph examination:

> Mr. Phalen. We have a reinvestigation program which is cyclical, and it is based as closely as we can make it on a 5-year cycle. In the course of that 5-year cycle we send out another questionnaire to the individual and ask him to update his

[48] U.S. Postal Service CIPI Reprint No. 128–72; retained in subcommittee files.

data. We also conduct a field investigation updating what we have in our security files. When all this is put together there is a determination whether or not this is something that would require a clarifying interview.

Now, this clarifying interview could be just a straight interview, just asking him, or it could be that we might think that a polygraph would be helpful, and also the individual occasionally thinks that a polygraph might be helpful, particularly where the information comes from an area where we can't reach by our investigative processes.

For example, some overseas areas where people do spend much of their lives.

This is getting to your question. We polygraph, I would say, no more than one to five people a year under that arrangement. So my short answer to your question is, we do not polygraph people as part of our reinvestigation program, that is, periodically. It is only at the time that something comes up in the course of reinvestigation which we feel requires clarification, or it would be helpful if we could clarify it. The number is almost minimal.

And second, I think we should stress that it is completely voluntary. We do have people who have said, I do not wish to take a reinvestigation polygraph. We have accepted this. We have asked them why. And they are all still employed, and there is no record of this in their personnel files or in their security files.

* * * * *

Mr. PHALEN. One of the reasons is—and it fits many of them—is that their career has been outstanding, and their life is relatively an open book. And, of course, in our relatively closed society of the intelligence community it is quite a bit of an open book. And on that basis they would prefer not to go through it. Of course, some of this is a hangover from questions that have been asked in the past which were a little too broad. Frankly, our earlier approaches to screening might have been a little too broad, and evoked responses in rather personal areas which we don't go into any more.

And this possibly is a feeling from that earlier time.

We have refined our questions down—and I can go into some examples there if we wish where we do not do that any more—this would be an example, that a person says he would rather not go through it. Occasionally they have touched on their own personal philosophy, the integrity of themselves. They would prefer not to subject themselves to this.[49]

AVAILABILITY OF RESULTS TO INDIVIDUALS TESTED

Individuals who are polygraphed by the CIA and NSA are not told of the findings and conclusions of the examiners. The State Department reports that only the general nature of the polygraph test

[49] Hearings, pp. 654–655. See footnote 5 on p. 3.

findings are made known to the individuals undergoing that type examination. The other four agencies which reported using this testing procedure in connection with criminal investigations gave answers slightly different, one from the other, and covered a fairly broad spectrum of practice.

In the Treasury Department, the Secret Service responded that:

> The findings of all such polygraph examinations would most definitely be made available to the subjects of such tests. Since this is a fundamental procedure in conducting the examination we can think of no single situation where this would not be done.

The U.S. Customs Bureau response was a simple "yes" to the same question. The U.S. Postal Service generally makes the examination's findings available to the individual being polygraphed. This is not required by its regulations, but this "policy" has, over a period of time, been communicated verbally to its polygraph examiners. The Justice Department does not disclose to the individual either the results of the polygraph tests or the examiner's final opinion based on test findings.

Reassurance that refusal to submit to the polygraph test will not result in stigma attaching to that individual, and that no record is made of that refusal in his official personnel file are comforting, in some degree. However, information provided the subcommittee by the Department of Treasury's U.S. Secret Service discloses that:

> * * * his or her refusal would merely be reflected as a comment in the criminal investigative file and not in any individual personnel record.[50]

Ten years earlier, when queried on this point, all Federal agencies responding reported that refusals by employees to take polygraph tests were not noted in their personnel records, although such matters might be mentioned in investigative reports. The information furnished on the administrative controls over the confidentiality of test results strongly indicates that the condition still persists.

Assurance of Confidentiality of Test Results

As previously indicated, polygraph test results are normally incorporated into substantive investigative files which are separate and apart from an individual's official personnel file. No agency incorporates the results of the polygraph tests into a computerized data bank nor is such data normally interchanged among Federal agencies. Where two or more agencies cooperate in a criminal investigation, particularly where the U.S. Postal Service and the Treasury Department are involved, there can be a sharing of information which includes polygraph test results. In most other reported circumstances, polygraph test results are not made known to other Federal agencies.

Both the U.S. Postal Service and the National Security Agency instructions make provision for release of this type of information

[50] Letter dated Nov. 2, 1973, retained in subcommittee files.

to outside agencies, with the approval of the Chief Postal Inspector on the one hand, and the NSA Director or Deputy Director, on the other.

Appeals of Polygraph Test Results

Policies and practices applicable to the appeal of polygraph test results have not changed substantially since the committee last reported on this subject. Several agencies reported that no administrative or criminal action is taken predicated solely on the basis of these examinations and that provision for appeal from adverse polygraph test results is therefore unnecessary. However, the agencies taking that position further noted that any adverse administrative action resulting from an inquiry or investigation would be subject to appeal under the agencies' normal adverse action appeals program.

Special Test Facilities

Three agencies reported that special examining rooms or other facilities are maintained for administering polygraph tests. The Treasury Department's Secret Service reports that its examining rooms have two-way mirrors and that some are equipped with recording devices. Examinees normally are told of the existence of both items. The special test rooms maintained by the CIA generally are not equipped with two-way mirrors, but do have a capability to monitor and record the audible portion of the test. The examinee is told whether the interview is being monitored or recorded, if he asks about it. The NSA special facilities for polygraph testing are equipped with two-way mirrors, and monitoring and/or recording devices. Agency instructions require that the examinee be told about these special characteristics of the test room prior to the examination.

IX. RECOMMENDATIONS

It is the recommendation of the committee that the use of polygraphs and similar devices be discontinued by all Government agencies for all purposes.

While recognizing that there has been substantial compliance with the committee recommendations of 1965 calling for increased uniformity of administration of the polygraph and comprehensive research into their validity and reliability, the clear import of the hearings upon which this report is based leads to the same conclusion as was reached in 1965. The conclusion at that time was that:

> There is no "lie detector," neither machine nor human. People have been deceived by a myth that a metal box in the hands of an investigator can detect truth or falsehood.

The Department of Justice continues to maintain the position that the results of polygraph examinations would not be admitted as evidence in the Federal courts. The committee adopts this position and further affirms that since such examinations are considered invalid for evidentiary purposes, there is absolutely no reason for continuing the use of such examinations for investigatory purposes.

Although there is indication that efforts are being made to upgrade the training and educational requirements of polygraph operators, the committee finds that unproven technical validity of the polygraph devices themselves makes such efforts a meaningless exercise.

Even if the committee adopted the positions of some agencies that the polygraph is useful solely as a secondary investigative technique and that the results of a polygraph examination alone are never considered conclusive, the committee finds that the inherent chilling affect upon individuals subjected to such examinations clearly outweighs any purported benefit to the investigative function of the agency.

The committee additionally recommends that the use and/or acquisition of other so-called "lie detectors" such as the PSE or the voice analyzer be discontinued. Evidence presented in the hearings upon which this report is based demonstrates that such devices have even less scientific validity than the polygraph. Although no agency of the Federal Government is using such other devices at this time as a substitute for polygraph examinations, the committee recommends that additional federally-funded research into such devices be discontinued.

APPENDIXES

Appendix A.—Questionnaire on Polygraphs and Psychological Stress Evaluators

1. Does your agency possess or make use of polygraphs or psychological stress evaluator detection devices? (If major subordinate organizations within your agency engage in such activity, please list all those organizations.)

2. How many polygraphs and psychological stress evaluator detection devices are the property of your agency? Your response should show separate data for each of these two categories of devices, if available.

(*a*) Please list the total acquisition cost of all such devices.

(*b*) Please estimate the total annual maintenance costs of such devices and indicate whether maintenance is performed by agency personnel or by outside sources.

(*c*) If your agency leases such devices, or contracts with other public or private agencies to perform such tests, please provide the total costs for such activity during fiscal 1973.

(*d*) Please estimate all additional expenses attributable to such testing, such as travel expenses for examiners to and from location of tests, internal and external training programs, and all other costs for fiscal 1973.

(*e*) Do you have on loan to or loan from other Federal agencies or any other sources any polygraphs or psychological stress evaluator detection devices? If yes, give the number of such devices and identify the agencies or sources involved.

3. Please provide two copies each of all intra-agency directives, administrative orders, rules, regulations, and/or instructions governing the use of such devices within your agency.

4. Briefly explain your agency's general procedures governing the use of both categories of devices and answer the following specific questions. (Please explain procedures and indicate if they are covered by regulation in connection with each question. If more than one major subordinate organization within the agency is affected, provide separate responses for each.)

(*a*) For what specific purposes are these devices used (i.e., employment interviews, security clearance processing, suspected improper conduct of duties, medical measurements, or other purposes. List in order of most frequent use.

(*b*) Are the devices used in every instance involving those purposes listed in answer to (*a*) above?

(*c*) What weight is given to the data resulting from tests by these devices, or refusals to take such tests in relation to other types of investigative information?

(*d*) Who makes the initial determination to use such devices, and is this initial determination subject to review by higher authority in each case?

(*e*) Is the physical and mental condition of each person to be tested considered to determine suitability to take such a test?

(*f*) What disposition is made of data derived from such tests given to persons connected with your agency (i.e., retained in affected individuals' personnel files, retained separately, entered into a computerized information system data bank, made available to other Government agencies, etc.).

(*g*) Are the findings of such tests made available to the subjects of such tests?

(*h*) Is there a right of appeal in cases of adverse findings?

(*i*) Is access to such data restricted and, if so, what classification or other designation is applied to the data?

(*j*) If a person connected with your agency refuses to take such a test, is that refusal reflected in any way whatsoever in the individual's personnel records?

(*k*) Does your agency maintain special facilities, such as specially designed rooms, for the performance of such tests? Briefly describe such facilities and how they are equipped, stating particularly if they have two-way mirrors and recording devices. Furnish photographs, if available.

APPENDIX B.—CORRESPONDENCE FROM FORMER CHAIRMAN MOORHEAD TO THE EXECUTIVE SECRETARY OF THE PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD

JUNE 7, 1974.

EXECUTIVE SECRETARY.
President's Foreign Intelligence Advisory Board, Executive Office Building, Washington, D.C.

DEAR SIR: This subcommittee has a long-standing and continuing concern with the subject of polygraph testing by Federal Government agencies of individuals being considered for employment. This practice of polygraph testing, as a prerequisite to employment, is one reserved to the agencies having highly sensitive intelligence or counterintelligence missions directly affecting the national security.

It would appear that the President's Foreign Intelligence Advisory Board would have such a mission. Accordingly, we would be interested in answers to the following questions:

1. Is appointment as a member of the Board contingent upon the designee taking and passing a polygraph test?

2. Is employment as the Executive Secretary or as staff to that individual contingent, in each case, upon the taking and passing of a polygraph test?

3. If the answer to either 1 or 2 above is affirmative, what organization gives the tests, and to whom are the test results reported?

4. If the requirement does exist, have all members currently serving on the Board or administratively supporting the Board passed such a test in the past five years?

With best regards,

Sincerely,

WILLIAM S. MOORHEAD, *Chairman.*

APPENDIX C.—CORRESPONDENCE FROM THE EXECUTIVE SECRETARY OF THE PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD TO FORMER CHAIRMAN MOORHEAD

THE WHITE HOUSE.
Washington, D.C., June 12, 1974.

Hon. WILLIAM S. MOORHEAD,
Chairman, Foreign Operations and Government Information Subcommittee of the Committee on Government Operations, Rayburn House Office Building, Washington, D.C.

DEAR CONGRESSMAN MOORHEAD: Following are answers to the questions raised in your letter of June 7:

1. Appointment as a member of the President's Foreign Intelligence Advisory Board (PFIAB) is not contingent upon passing a polygraph test.

2. Appointment as the Executive Secretary or employment on the PFIAB staff is not contingent upon passing a polygraph test.

Should you have any further questions, please do not hesitate to contact me.

With kindest regards.

WHEATON B. BYERS, *Executive Secretary.*

(50)

SEPARATE VIEWS OF HON. SAM STEIGER (CONCURRED IN BY HON. FRANK HORTON, HON. JOHN N. ERLENBORN, HON. JOHN W. WYDLER, HON. CLARENCE J. BROWN, HON. GARRY BROWN, HON. CHARLES THONE, HON. EDWIN B. FORSYTHE, AND HON. ELLIOTT H. LEVITAS)

The recommendations contained in this report for an absolute ban on the use of polygraphs and similar devices are contrary to the testimony presented at the hearings on which this report is based. It is our opinion that the testimony and discussions contained in this report support the original recommendations agreed upon earlier by the Subcommittee on Government Information and Individual Rights. We think they should be made a part of this report with particular reference to recommendation No. 2.

Recommendations

No. 1

The committee has not changed its basic views about the benefits of and the need for research relative to polygraphs, and it has similar views relative to psychological stress evaluators, voice analyzers, and other types of stress-measuring instruments. Testimony developed during recent hearings showed that a number of Federal agencies are either conducting in-house research or are funding such research through contracts.

The committee recommends, because the applicable technology and the related scientific disciplines are so specialized, that insofar as Federal agencies fund further research in this area, a more formal and organized approach be developed for any such research, so that the different projects complement one another. This could preclude or minimize the possibility of duplicative or concurrent research, provide an effective mechanism for sharing research findings and conclusions having common applicability, and better recognize any given agency's unique requirements.

No. 2

The committee strongly reaffirms its earlier position with respect to the use of polygraphs, and recommends that the use of polygraphs and other stress evaluator devices by Federal agencies be prohibited in all cases but (1) those clearly involving the Nation's security and (2) those in which agencies can demonstrate in compelling terms their need for use of such devices for their law enforcement purposes, and that such uses would not violate the fifth amendment or any other provision of the Constitution.

No. 3

The committee recommends that the pertinent sections of the CSC's Federal Personnel Manual be revised to give visibility and emphasis to an individual's rights and alternatives when he is requested to submit to a polygraph test. The Commission's regulations should address themselves specifically not only to the approval uses of polygraph tests to pre-employment screening situations but also to those situations in which the question of the continuance of an individual's employment in a competitive service position is under consideration or at issue because questions may have arisen about his honesty or the propriety of his conduct.

The committee also sees a need for and recommends to the Civil Service Commission that it require agencies each year to report the number of polygraph tests given to competitive service and to excepted employees, the reasons for those tests, and the uses made of the results of the tests.

No. 4

The committee recommends that the Department of Defense give additional consideration to a cross-service arrangement among its many components for polygraph testing, so that the overall requirements for devices and for training polygraph examiners might be reduced, with resulting savings to the Government.

The committee hesitates to recommend that some Government-wide central monitoring and control point be established for the purchase and test evaluation of PSE's and voice analyzers solely on the basis of their acquisition cost. However, the ancillary costs involved in uncoordinated, multi-organization contracting for or in-house performance of evaluation tests can easily become significant, as is evidenced by what is happening in the Department of Defense. For that reason, the committee does recommend that the Department of Defense establish a single point of management for those devices and other newly developed similar devices represented as being useful as lie detectors to satisfy that agency's stated needs.

No. 5

Discerning between "truth" and "deception" is the stated objective of the polygraph operator; therefore, his ability to do so should not be dependent in any way upon the special mission responsibilities of his employing agency. It follows then that all polygraph examiners should be equally well-trained and qualified. The committee accordingly recommends that a common set of qualifications (educational training, experience and personal) be established for polygraph examiners of all Federal agencies. Both in education and training, the committee recommends that the requirements for a baccalaureate-level education and special training as a polygraph examiner give greater emphasis to the fields of psychology, physiology, and behavioral sciences.

The marked variations in the duration of the special formal training given by different agencies to polygraph examiners needs further

consideration. The committee particularly recommends that the Department of Defense critically reassess its earlier justifications for expanding its formal training course from the original period of 8 weeks to the present 14 weeks training course. Such an evaluation should, at the very least, examine and compare the content of the Army school's syllabus with the training syllabuses of those agencies which give their formal training in periods of 6 to 7 weeks. If those other training course curriculums are found to be adequate, then DOD should take the necessary steps to shorten its polygraph training courses.

The advantages of uniformity and economy that normally would accrue if all Federal agency polygraph examiners were given their highly specialized basic training at a single, adequately equipped facility appear self-evident to the committee. It therefore recommends to those other Federal agencies which contract for or operate such in-house training programs that they begin discussions with DOD about having their employees trained at the Army's Military Police School, Fort Gordon, Ga., on a cost-reimbursable basis.

No. 6

It is the belief of the committee that attitudinal changes in recent years are evidenced in the greater concern shown by Federal agencies about the manner and conditions under which polygraph tests are given and about the confidentiality accorded and the uses being made of the polygraph test results.

The organizational levels at which requests for polygraph testing must be approved, on a case-by-case basis, are gratifyingly high. Assurances that the test results, by themselves, are only another matter for consideration, rather than the sine qua non upon which personnel decisions are made by agencies, also are gratifying. On the other hand, the fact that refusal to submit to polygraph testing remains a bar to initial employment by CIA and NSA is hardly justifiable, in the committee's view, merely because of the "national security" claim advanced by these two agencies. A number of other agencies also have sensitive missions but do not require pre-employment polygraphing.

There still are a number of marked differences in the Federal agencies' practices that relate to equipping special test rooms and disclosing to the examinee the results of the polygraph tests.

The committee remains persuaded that determining whether or not an individual's state of mental and physical health is acceptable, before he undergoes a polygraph test, is a decision that should be made by properly trained medical professionals rather than by polygraph examiners.

The committee's recommendation of a decade ago, that all Government agencies be placed under a uniform administrative system which would enforce maximum controls on the use of polygraphs and which would establish regulations to prevent their proliferation and misuse, appears to have been accepted and acted upon, to a considerable degree. There is, however, substantial opportunity to make more uniform a number of the agency practices referred to above. To accomplish this, the committee recommends that the President reestablish an interagency committee to consider these matters, to act as a clearinghouse

of agencies' research activities involving polygraph and other stress analysis devices, and to coordinate the periodic reporting recommended earlier in this report.

SAM STEIGER.

We concur in the foregoing views:

FRANK HORTON.
JOHN N. ERLENBORN.
JOHN W. WYDLER.
CLARENCE J. BROWN.
GARRY BROWN.
CHARLES THONE.
EDWIN B. FORSYTHE.
ELLIOTT H. LEVITAS.

DISSENTING VIEWS OF HON. FRANK HORTON, HON. CLARENCE J. BROWN, HON. PAUL N. McCLOSKEY, JR., HON. JOEL PRITCHARD, HON. JOHN N. ERLENBORN, HON. CHARLES THONE, HON. GARRY BROWN, HON. EDWIN B. FORSYTHE, HON. ALAN STEELMAN, HON. ROBERT W. KASTEN, JR., HON. SAM STEIGER, HON. JOHN W. WYDLER, AND HON. WILLIS D. GRADISON, JR.

We disagree strongly with the recommendation made at the conclusion of this Report, that the use of polygraphs and similar devices be discontinued by all government agencies for all purposes.

The factual information and opinions referred to in the Report relate solely to hearings held in June, 1974, *during an entirely different Congress*, and participated in by an entirely different group of Members. There were two days of hearings in 1974. On June 4, the Hearing Record discloses that five Members were present: then-Chairman William Moorhead, Bill Alexander and James Stanton, Democrats, and John Erlenborn and Ralph Regula, Republicans. The following day, June 5th, only Mr. Moorhead and Mr. Erlenborn were in attendance. None of these members serve on the Subcommittee in this, the 94th Congress, which proposed this Report. None who *do* serve at the present time on the Subcommittee were present or participated in the 1974 hearings.

The testimony and subsequent statements received for inclusion in the 1974 record take up 790 pages and represent a wide diversion of views and suggestions. *No* witness, however, urged prohibition of the polygraph for all purposes as the Committee majority now recommends.

Even the ACLU and the American Federation of Government Employees did not go this far. Former Senator Sam Ervin submitted perhaps the most persuasive argument, that no American be compelled to submit to polygraph testing as a condition of obtaining or retaining federal employment.

A majority of us who join in these dissenting views agree with Senator Ervin. But this is a far cry from recommending that the government be prohibited from use of the polygraph for all purposes. What of the individual under investigation in a doubtful case who asks that he be tested in order to try to prove his innocence? Is this privilege one which our government should deny him? We think not.

While we have grave reservations about the use of the polygraph in 1973 by DOD and the CIA as disclosed in the 1974 testimony, there is

absolutely nothing in the hearing record to justify the recommendation made by the Committee majority.

How, then, did the Committee reach such recommendation?

The answer provides an interesting commentary on congressional procedures. First, it should be noted that an earlier draft report was prepared in March, 1975, to reflect the record of the 1974 hearings. That report, prepared for submission to the full Committee at its April meeting, included at page 20, the specific recommendation that polygraph tests should be . . .

> prohibited in all cases, but (1) those clearly involving the National Security and (2) those in which agencies can demonstrate in compelling terms their need for use of such devices for their law enforcement purposes and that such uses would not violate the fifth amendment or any other provision of the Constitution.

There were five other specific recommendations as to the use of polygraphs, but *none* which suggested that they be prohibited absolutely.

The recommendations of the draft report were approved by the Subcommittee in March 1975, (with four Members, Chairwoman Abzug, Ranking Minority Member, Sam Steiger, Andrew Maguire, and Paul McCloskey participating in the meeting) and ordered reported to the full Committee on Government Operations on March 25, 1975.

Six recommendations were thus approved. They were based on a careful review of the testimony at the 1974 hearings, and both the Chairwoman and two of the three Republicans on the Subcommittee concurred in these recommendations.

Thereafter, however, the two Subcommittee staff members who prepared the report, James Kronfeld and Nancy Wenzel, were replaced by the Chairwoman with five new staff members, *none* of whom had participated in the 1974 hearings or in the preparation of the March draft report.

The Chairwoman thereafter did not comply with the March 25 vote of her Subcommittee and did not submit the draft report to the full Committee. Instead, she waited until September 25, six months later, at which time she circulated a memorandum to the Subcommittee on another subject, (the National Women's Conference bill) and adding a single sentence to the end that there would also be consideration of a revised recommendation on the polygraph Report.

No arguments were submitted in support of this change of recommendations and at a hurried meeting on September 30, 1975, attended by six Members of the Majority, but with no Minority Members present and *without either discussion or debate*, the new recommendation was adopted in a 6 to 0 vote by Subcommittee Members, *none of whom* had participated in the 1974 hearings or the preparation of the earlier draft Report approved by the Subcommittee in March, 1975.

It seems to us that this procedure is both demeaning to the House as well as indicative of a certain lack of validity in the recommendation.

Our own recommendations remain the original recommendations of the March 25, 1975 draft Report which follows:

1. The committee has not changed its basic view about the benefits of and the need for research relative to polygraphs, and it has similar views relative to psychological stress evaluators, voice analyzers, and other types of stress-measuring instruments. Testimony developed during recent hearings showed that a number of Federal agencies are either conducting in-house research or are funding such research through contracts.

The committee recommends, because the applicable technology and the related scientific disciplines are so specialized, that insofar as Federal agencies fund further research in this area, a more formal and organized approach be developed for any such research, so that the different projects complement one another. This could preclude or minimize the possibility of duplicative or concurrent research, provide an effective mechanism for sharing research findings and conclusions having common applicability, and better recognize any given agency's unique requirements.

2. The committee strongly reaffirms its earlier position with respect to the use of polygraphs, and recommends that the use of polygraphs and other stress evaluator devices by Federal agencies be prohibited in all cases but (1) those clearly involving the Nation's security and (2) those in which agencies can demonstrate in compelling terms their need for use of such devices for their law enforcement purposes, and that such uses would not violate the fifth amendment or any other provision of the Constitution.

3. The committee recommends that the pertinent sections of the CSC's Federal Personnel Manual be revised to give visibility and emphasis to an individual's rights and alternatives when he is requested to submit to a polygraph test. The Commission's regulations should address themselves specifically not only to the approved uses of polygraph tests to preemployment screening situations but also to those situations in which the question of the continuance of an individual's employment in a competitive service position is under consideration or at issue because questions may have arisen about his honesty or the propriety of his conduct.

The committee also sees a need for and recommends to the Civil Service Commission that it require agencies each year to report the number of polygraph tests given to competitive service and to excepted employees, the reasons for those tests, and the uses made of the results of the tests.

79-064 O - 76 - 14

4. The committee recommends that the Department of Defense give additional consideration to a cross-service arrangement among its many components for polygraph testing, so that the overall requirements for devices and for training polygraph examiners might be reduced, with resultant savings to the Government.

The committee hesitates to recommend that some Government-wide central monitoring and control point be established for the purchase and test evaluation of PSE's and voice analyzers solely on the basis of their acquisition cost. However, the ancillary costs involved in uncoordinated, multi-organizational contracting for or in-house performance of evaluation tests can easily become significant, as is evidenced by what is happening in the Department of Defense. For that reason, the committee does recommend that the Department of Defense establish a single point of management for those devices and other newly developed similar devices represented as being useful as lie detectors to satisfy that agency's stated needs.

5. Discerning between "truth" and "deception" is the stated objective of the polygraph operator; therefore, his ability to do so should not be dependent in any way upon the special mission responsibility of his employing agency. It follows then that all polygraph examiners should be equally well-trained and qualified. The committee accordingly recommends that a common set of qualifications (educational training, experience and personal) be established for polygraph examiners of all Federal agencies. Both in education and training, the committee recommends that the requirement for a baccalaureate-level education and special training as a polygraph examiner give greater emphasis to the fields of psychology, physiology, and behavioral sciences.

The marked variations in the duration of the special formal training given by different agencies to polygraph examiners needs further consideration. The committee particularly recommends that the Department of Defense critically reassess its earlier justifications for expanding its formal training course from the original period of 8 weeks to the present 14 weeks training course. Such an evaluation should, at the very least, examine and compare the content of the Army school's syllabus with the training syllabuses of those agencies which give their formal training in periods of 6 to 7 weeks. If those other training course curriculums are found to be adequate, then DOD should take the necessary steps to shorten its polygraph training course.

The advantages of uniformity and economy that normally would accrue if all Federal agency polygraph examiners were given their highly specialized basic training at a single, adequately equipped facility appear self-evident to the com-

mittee. It therefore recommends to those other Federal agencies which contract for or operate such in-house training programs that they begin discussions with DOD about having their employees trained at the Army's Military Police School, Fort Gordon, Ga., on a cost-reimbursable basis.

6. It is the belief of the committee that attitudinal changes in recent years are evidenced in the greater concern shown by Federal agencies about the manner and conditions under which polygraph tests are given and about the confidentiality accorded and the uses being made of the polygraph test results.

The organizational levels at which requests for polygraph testing must be approved, on a case-by-case basis, are gratifyingly high. Assurances that the test results, by themselves, are only another matter for consideration, rather than the sine qua non upon which personnel decisions are made by agencies, also are gratifying. On the other hand, the fact that refusal to submit to polygraph testing remains a bar to initial employment by CIA and NSA is hardly justifiable, in the committee's view, merely because of the "national security" claim advanced by these two agencies. A number of other agencies also have sensitive missions but do not require preemployment polygraphing.

There still are a number of marked differences in the Federal agencies' practices that relate to equipping special test rooms and disclosing to the examinee the results of the polygraph tests.

The committee remains persuaded that determining whether or not an individual's state of mental and physical health is acceptable, before he undergoes a polygraph test, is a decision that should be made by properly trained medical professionals rather than by polygraph examiners.

The committee's recommendation of a decade ago, that all Government agencies be placed under a uniform administrative system which would enforce maximum controls on the use of polygraphs and which would establish regulations to prevent their proliferation and misuse, appears to have been accepted and acted upon, to a considerable degree. There is, however, substantial opportunity to make more uniform a number of the agency practices referred to above. To accomplish this, the committee recommends that the President reestablish an interagency committee to consider these matters, to act as a clearinghouse of agencies' research activities involving polygraph and other stress analysis devices, and to coordinate the periodic reporting recommended earlier in this report.

To show how the Committee reached a contrary view, we attach as Appendix A Chairwoman's memorandum of September 25, 1975.

60

Appendix A

U.S. House of Representatives,
Government Information and Individual Rights
Subcommittee, Committee on Government Operations,
Washington, D.C., September 25, 1975.

To: Members of the Government Information and Individual Rights Subcommittee.
From: Bella S. Abzug, Chairwoman.
Subject: Hearing on National Women's Conference Bill—Correction

Because of the Democratic Caucus called for 9:00 a.m. next Tuesday, September 30, the legislative hearing scheduled to consider H.R. 8903 (a bill to organize and convene a 1976 National Women's Conference) will be moved to 10:00 a.m., or shortly thereafter, and will start immediately following the conclusion of the Democratic Caucus.

The hearing will be held in the same room as scheduled, Room 2247 of the Rayburn House Office Building. Vote and mark-up of the bill will take place immediately after witness presentations at the hearing. If for any reason a quorum is not present at that time, mark-up will take place on Wednesday, October 1, at 2:00 p.m. in Room H–310, The Capitol.

Also to be voted on at the Tuesday hearing is the enclosed committee report on the use of polygraphs by federal agencies, and the revised recommendation.

Enclosures.

Polygraph Report: Errata Sheet

1. Pages 14, 20, 25, 33, 40, 48 and 49: strike out all portions headed "RECOMMENDATION" OR "RECOMMENDATIONS".

2. Page 49, after end of all text: insert the following new section:

IX. RECOMMENDATIONS

It is the recommendation of the committee that the use of polygraphs and similar devices be discontinued by all government agencies for all purposes.

While recognizing that there has been substantial compliance with the committee recommendations of 1965 calling for increased uniformity of administration of the polygraph and comprehensive research into their validity and reliability, the clear import of the hearings upon which this report is based leads to the same conclusion as was reached in 1965. The conclusion at that time was that:

> There is no "lie detector," neither machine nor human. People have been deceived by a myth that a metal box in the hands of an investigator can detect truth or falsehood.

The Department of Justice continues to maintain the position that the results of polygraph examinations would not be admitted as evidence in the Federal courts. The committee adopts this position and further affirms that since such examinations are considered invalid for

evidentiary purposes, there is absolutely no reason for continuing the use of such examinations for investigatory purposes.

Although there is indication that efforts are being made to upgrade the training and educational requirements of polygraph operators, the committee finds that unproven technical validity of the polygraph devises themselves makes such efforts a meaningless exercise.

Even if the committee adopted the position of some agencies that the polygraph is useful as a secondary investigative technique and that the results of a polygraph examination alone are never considered conclusive, the committee finds that the inherent chilling affect upon individuals subjected to such examinations clearly outweighs any purported benefit to the investigative function of the agency.

The committee additionally recommends that the use and/or acquisition of other so-called "lie detectors" such as the PSE or the Voice Analyzer be discontinued. Evidence presented in the hearings upon which this report is based demonstrates that such devices have even less scientific validity than the polygraph. Although no agency of the Federal government is using such other devices at this time as a substitute for polygraph examinations, the committee recommends that additional federally-funded research into such devices be discontinued.

Frank Horton.
Clarence J. Brown.
Paul N. McCloskey, Jr.
Joel Pritchard.
John N. Erlenborn.
Charles Thone.
Garry Brown.
Edwin B. Forsythe.
Alan Steelman.
Robert W. Kasten, Jr.
Sam Steiger.
John W. Wydler.
Willis D. Gradison, Jr.

[From the Congressional Record—House, Sept. 12, 1974]

Report of the Republican Task Force on Privacy

The Speaker pro tempore. Under a previous order of the House, the gentleman from California (Mr. Goldwater) is recognized for 30 minutes.

Mr. Goldwater. Mr. Speaker, it is with a good deal of pride and optimism that I take this time to announce to my colleagues that on August 21, 1974, the Republican Task Force on Privacy, of the Republican Research Committee, issued its report. It was a day of note for the people of the United States, the Congress, and the Republican Party. This report is the first and most comprehensive statement on the general subject of privacy issued by either party, or by any congressional committee.

Serving on the task force with me—and, I might add, making this task force far more than just another study group—were Tennyson Guyer and Alan Steelman, who served as cochairmen: John Conlan, Margaret Heckler, Andrew Hinshaw, Frank Horton, Jack Kemp, Robert Lagomarsino, John Rousselot, Keith Sebelius, and Charles Thone.

Each Member contributed fully and directly to the preparation of a specific section of the report, and had a hand in the report's total preparation. My fellow Republican colleagues and the entire House can be proud of their efforts and of their product. They have made a valuable contribution to our legislative process, and if the recommendations are implemented, to our quality of life.

I commend the report to my colleagues, and include its covering letter from Congressman Lou Frey, chairman of the Republican Research Committee, for your attention and consideration.

August 21, 1974.

Republican Research Committee,
Republic Conference, U.S. House of Representatives, Washington, D.C.

Dear Republican Colleague: Attached are the recommendations of the Task Force on Privacy, chaired by Barry M. Goldwater, Jr., and Vice-chaired by Alan Steelman and Tennyson Guyer. Other Members of the Task Force are John Conlan, Charles Thone, Jack Kemp, Peggy Heckler, Andrew Hinshaw, Frank Horton, Charles Mosher, Bob Lagomarsino, John Rousselot, and Keith Sebelius.

These recommendations are a landmark in the area of individual rights. Nowhere has the total question of privacy been so well or thoughtfully covered. Nowhere has the human equation in our technological society been so strongly expressed.

The Research Committee is proud to have approved this report. These recommendations and the follow-up legislative efforts will ensure that the 1984 envisioned by George Orwell will remain only fictional.

The Task Force and its staff, especially Joe Overton, are to be commended for the time, effort and excellence of the product.

Most sincerely,

Lou Frey, Jr.

August 21, 1974.

House Republican Research Committee: Recommendations of Privacy Task Force

The House Republican Research Committee has approved the following recommendations of the Task Force on Privacy which deal with the following areas:

Government surveillance, Federal information collection, social security numbers/standard universal identifiers, census information, financial information, consumer reporting, school records, juvenile records, arrest records, medical records, computer data banks, and code of ethics.

The House Republican Task Force on Privacy believes that the right to privacy is an issue of paramount concern to the nation, the public and the Congress. Recently publicized incidents of abuses have begun to focus attention on this long neglected area. Public awareness must be heightened and the legislative process geared up to address the full range of problems posed by the issue.

Modern technology has greatly increased the quantity and detail of personal information collection, maintenance, storage, utilization and dissemination. The individual has been physically by-passed in the modern information process. An atmosphere exists in which the individual, in exchange for the benefit or service he obtained, is assumed to waive any and all interest and control over the information collected about him. On the technical and managerial levels, the basic criteria in many decisions relating to personal information practices are considerations of technological feasibility, cost-benefit and conveniences. The right to privacy has been made subservient to concerns for expediency, utility and pragmatism.

The trend in personal information practices shows no signs of abating. Twice as many computer systems and seven times as many terminals—particularly remote terminals—will be in use by 1984 as are in use today. And, with each federal service program that is initiated or expanded, there is a geometrically proportionate increase in the quantity and detail of personal information sought by the bureaucracy. The theory is that the broader the information base, the more efficient and successful the administration of the program.

Such a situation demands the attention of Congress and of the American public. The computer does not by definition mean injury to individuals. Its presence has greatly contributed to the American economy and the ability of government to serve the people. Under present procedures, however, the American citizen does not have a clearly defined right to find out what information is being collected, to see such information, to correct errors contained in it, or to seek legal redress for its misuse. Simply put, the citizen must continue to give out large quantities of information but cannot protect himself or herself from its misappropriation, misapplication or misuse. Both government and private enterprise need direction, because many of their practices and policies have developed on an isolated, ad hoc basis.

The House Republican Task Force on Privacy has investigated the following general areas involving the investigation and recording of

personal activities and information: government surveillance, federal information collection, social security numbers and universal identifiers, census information, bank secrecy, consumer reporting, school records, juvenile records, arrest records, medical records, and computer data banks. These inquires have resulted in the development of general suggestions for legislative remedies. Each statement is accompanied by a set of findings.

All findings and recommendations are presented with the intent of being consistent with these general principles:

1. there should be no personal information system whose existence is secret;

2. information should not be collected unless the need for it has been clearly established in advance;

3. information should be appropriate and relevant to the purpose for which it has been collected;

4. information should not be obtained by illegal, fraudulent, or unfair means;

5. information should not be used unless it is accurate and current;

6. procedures should be established so that an individual knows what information is stored, the purpose for which it has been recorded, particulars about its use and dissemination, and has the right to examine that information;

7. there should be a clearly prescribed procedure for an individual to correct, erase or amend inaccurate, obsolete, or irrelevant information;

8. any organization collecting, maintaining, using, or disseminating personal information should assure its reliability and take precautions to prevent its misuse;

9. there should be a clearly prescribed procedure for an individual to prevent personal information collected for one purpose from being used for another purpose without his consent;

10. the Federal Government should not collected personal information except as expressly authorized by law; and

11. that these basic principles apply to both governmental and non-governmental activities.

Each recommendation of the Task Force seeks to contribute to a broader, more intelligent, viable understanding of the need for a renewed concern for personal privacy. An awareness of personal privacy must be merged with the traditional activities of the free marketplace, the role of government as a public servant, and the need for national security, national defense, and foreign affairs.

SURVEILLANCE

The Task Force is deeply disturbed by the increasing incidence of unregulated, clandestine government surveillance based solely on administrative or executive authority. Examples of such abuses include wiretapping, bugging, photographing, opening mail, examining confidential records and otherwise intercepting private communications and monitoring private activities. Surveillance at the federal level receives the most publicity. However, state and local government, military intelligence and police activities also must be regulated.

The Fourth Amendment of the Constitution clearly specifies "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." The First Amendment guards against abridgement of the rights of free speech, free press, and assembly for political purposes. The Fourteenth Amendment states that none of a citizen's rights may be taken from him by governmental action without the due process of law.

The direct threat to individual civil liberties is obvious in those cases in which a person is actually being monitored, but even more alarming is the "chilling effect" such activities have on all citizens. A person who fears that he will be monitored may, either subconsciously or consciously, fail to fully exercise his constitutionally guaranteed liberties. The mere existence of such fear erodes basic freedoms and cannot be accepted in a democratic society.

The various abuses of discretionary authority in the conduct of surveillance provide ample evidence that current safeguard mechanisms do not work. Procedures allowing the executive branch to determine whether a surveillance activity is proper or not pose certain conflict of interest questions.

A degree of controversy surrounds the question of the authority of the President to initiate electronic surveillance without the safeguards afforded by court review. Present law is clear on this point: the Omnibus Crime Control and Safe Streets Act of 1968 lists those specific crimes in connection with which electronic monitoring may be instituted and requires that court approval be obtained in these cases. However, dispute has arisen over Executive claims of Constitutional prerogatives to implement wiretaps for national security purposes. The Supreme Court has ruled that, if such prerogative exists, it does not apply to cases of domestic surveillance unrelated to national security. The Court has not yet ruled on the constitutionality of national security wiretaps unauthorized by a court. Cases are pending before the courts at this time which raise this issue. The Task Force agrees with the movement of the Judiciary to circumscribe unauthorized wiretaps and hopes it will proceed in this direction.

The Task Force feels that surveillance is so repugnant to the right to individual privacy and due process that its use should be confined to exceptional circumstances. The Task Force further feels that no agent of federal, state, or local government should be permitted to conduct any form of surveillance, including wiretapping of U.S. citizens in national security cases, without having demonstrated probable cause and without having obtained the approval of a court of competent jurisdiction. The Task Force recommends enactment of new legislation to prohibit the unauthorized surveillance by any means, and further recommends that existing laws be clarified to the extent this may be necessary to ensure that no agent of the government, for any reason, shall have the authority to conduct any surveillance on any American citizen for any reason without first obtaining a court order.

The Task Force believes that this proposal would not lessen the capability of the government to protect and defend the American people, but would go a long way toward assuring the individual citizen that his constitutional rights will not be abridged by government without due process of law.

FEDERAL INFORMATION COLLECTION

Recently, there has been a pronounced increase in federal data and information collection. Over 11.5 million cubic feet of records were stored in Federal Records Centers at the beginning of FY 1973. Accompanying this increase has been a rise in the potential for abuse of federal information collection systems.

The Federal Reports Act of 1942 was enacted to protect individuals from overly burdensome and repetitive reporting requirements. The agency entrusted with the responsibility for implementing the Act has ignored the legislative mandate and failed to hold a single hearing or conduct any investigations. With the exception of the Bureau of the Census and the Internal Revenue Service, there are few restrictions on the collection or dissemination of confidential information compiled by federal agencies.

The Task Force recommends that the Office of Management and Budget immediately begin a thorough review and examination of all approved government forms and eliminate all repetitive and unnecessary information requirements.

Legislation setting down clear guidelines and spelling out restrictions is needed to protect the individual from unrestricted and uncontrolled information collection. Individuals asked to provide information must be apprised of its intended uses. Individuals supplying information which will be made public must be notified of that fact at the time the information is collected or requested. Public disclosure (including dissemination on an intra- or inter-agency basis) of financial or other personal information must be prohibited to protect the privacy of respondents.

SSN/SUI

Returning the use of the Social Security Number (SSN) to its intended purpose (i.e. operation of old-age, survivors, and disability insurance programs) is a necessary corollary to safeguarding the right of privacy and curtailing illegal or excessive information collection.

The use of the Social Security Number has proliferated to many general items including state driver licenses, Congressional, school and employment identification cards, credit cards and credit investigation reports, taxpayer identification, military service numbers, welfare and social services program recipients, state voter registration, insurance policies and records and group health records.

There are serious problems associated with the use of the SSN as a standard universal number to identify individuals. A standard universal identifier (SUI) will relegate individuals to a number; thereby, increasing feelings of alienation. The SSN's growing use as an identifier and filing number is already having a negative, dehumanizing effect upon many citizens. In addition, the use of a SUI by all types of organizations enables the linking of records and the tracking of an individual from cradle to grave. This possibility would negate the right to make a "fresh start", the right of anonymity, and the right to be left alone, with no compensating benefit.

A well-developed SUI system would require a huge, complex bureaucratic apparatus to control it and demand a strict system of professional ethics for information technicians. The technology

needed to protect against unauthorized use has not yet been adequately researched and developed. A loss, leak or theft would seriously compromise a system and official misappropriation could become a political threat. The following Congressional action is needed:

1. legislation should be enacted that sets guidelines for use of the SSN by limiting it to the operation of old-age, survivors, and disability insurance programs or as required by federal law;

2. any Executive Orders authorizing federal agencies to use SSN's should be repealed, or alternatively, reevaluated and modified;

3. legislation should be enacted restricting the use of the SSN to well-defined uses, and prohibiting the development and use of any type of SUI until the technical state of the computer can ensure the security of such a system. At that time, a SUI system should have limited applicability and should be developed only after a full congressional investigation and mandate; and

4. new government programs should be prohibited from incorporating the use of the SSN or other possible SUI. Existing programs using the SSN without specific authorization by law must be required to phase out their use of the SSN. State and local governmental agencies, as well as the private sector, should follow this same course of action.

A review should be conducted of the Internal Revenue Service in both its collection and dissemination policies. Leaks must be ended. The need for stricter penalties for unauthorized activities should be reviewed.

CENSUS BUREAU

The greatest personal data collection agency is the Bureau of Census. Created to count the people in order to determine congressional districts, this agency has mushroomed into a vast information center which generates about 500,000 pages of numbers and charts each year.

Under penalty of law, the citizen is forced to divulge intimate, personal facts surrounding his public and private life and that of the entire family. These answers provide a substantial personal dossier on each American citizen. The strictest care must be taken to protect the confidentiality of these records and ensure that the in * * *.

The Census Bureau sells parts of its collected data to anyone who wishes to purchase such information. Included are all types of statistical data that are available on population and housing characteristics. As the questions become more detailed and extensive, broad-scaled dissemination becomes more threatening, and frightening. When used in combination with phone directories, drivers' licenses and street directories, census data may enable any one interested to identify an individual. Therefore, it is vitally important that rules and regulations governing the access to and dissemination of this collected data be reviewed, clarified and strengthened.

Legislation is needed to guarantee the confidentiality of individual information by expanding the scope of confidentiality under existing law and by increasing the severity of punishment for divulging confidential information. These provisions should be specifically directed at the officers and employees of the Bureau of Census, all officers and

employees of the Federal Government and private citizens who wrongfully acquire such information. In addition, the Bureau of the Census must use all available technological sophistication to assure that individuals cannot be inductively identified.

FINANCIAL INFORMATION

On October 26, 1970, sweeping legislation known as the Bank Secrecy Act became law. The Act's intention was to reduce white collar crime by making records more accessible to law enforcement officials. However, in accomplishing its purpose, it allowed Federal agencies to seize and secure certain financial papers and effects of bank customers without serving a warrant or showing probable cause. The Act's compulsory recordkeeping requirements, by allowing the recording of almost all significant transactions, convert private financial dealings into the personal property of the banks. The banks become the collectors and custodians of financial records which, when improperly used, enable an individual's entire life style to be tracked down.

The general language of the Act allowed bureaucrats to ignore the intent of the law and neglect to institute adequate privacy safeguards. The Supreme Court affirmed this approach by upholding the constitutionality of both the law and the bureaucratic misinterpretations of it.

Congress must now take action to prevent the unwarranted invasion of privacy by prescribing specific procedures and standards governing the disclosure of financial information by financial institutions to Federal officials or agencies. Congress must enact legislation to assure that the disclosure of a customer's records will occur only if the customer specifically authorizes a disclosure or if the financial institution is served with a court order directing it to comply. Legislation must specify that legal safeguards be provided requiring that the customer be properly notified and be provided legal means of challenging the subpoena or summons.

Passage of such legislation would be an important step forward in reaffirming the individual's right to privacy.

CONSUMER REPORTING

The consumer reporting industry, through its network of credit bureaus, investigative agencies, and other reporting entities is in growing conflict with individual privacy. Most Americans eventually will be the subject of a consumer report as a result of applying for credit, insurance, or employment. The problem is one of balancing the legitimate needs of business with the basic rights of the individual.

Consumer reports fall into two categories. First, there are the familiar which contain "factual" information on an individual's credit record such as where accounts are held and how promptly bills are paid. 100 million consumer reports are produced each year by some 2600 credit bureaus.

The second ones go beyond factual information to include subjective opinions of the individual's character, general reputation, personal characteristics, and mode of living. These are often obtained through

interviews with neighbors, friends, ex-spouses and former employers or employees. An estimated 30 to 40 million such reports are produced annually.

The first Federal attempt at regulating the collection and reporting of information on consumers by third-party agencies came in 1970 with the enactment of the Fair Credit Reporting Act (FCRA). In theory, the Act had three main objectives: to enable consumers to correct inaccurate and misleading reports; to preserve the confidentiality of the information; and to protect the individual's right to privacy.

The specific safeguards provided by the FCRA are: A consumer adversely affected because of information contained in a consumer report must be so notified and given the identity of the reporting agency. The consumer is entitled to an oral disclosure of the information contained in his file and the identity of its recipients. Items disputed by the consumer must be deleted if the information cannot be reconfirmed. The consumer may have his version of any disputed item entered in his file and included in subsequent reports.

The FCRA needs to be strengthened in two major areas: disclosure requirements and investigative reports. The individual should be entitled to actually see and inspect his file, rather than rely on an oral presentation. Further, he should be allowed to obtain a copy of it by mail (the consumer is often geographically distant from the source of the file). Users of consumer reports should be required to specifically identify the information which triggered any adverse action.

The FCRA protects the sources used in investigative reports. The Task Force believes that this is contrary to the basic tenets of our system of justice and that the information source must be revealed upon the subject's request. Furthermore, the Task Force recommends that advance written authorization be required from any individual who is the subject of an investigative report for any purpose.

SCHOOL RECORDS

The recent increase in popular awareness of the seriousness of the privacy issue has been accompanied by an increase in the general concern over loose, unstructured and unsupervised school recordkeeping systems and associated administrative practices. There has also been general discussion about what information should be kept on a child and considered part of his or her "record". Parents are frequently denied access to their own child's record, or are prohibited from challenging incorrect or misleading infomation contained in his file. At the same time, incidents of highly personal data being indiscriminately disseminated to inquirers unconnected with the school system are not uncommon.

Remedial measures are available to the Congress in the form of legislative actions. The sanctions under which such provisions would operate, however, are the key to their effectiveness. The Task Force proposes the Congress adopts as a general policy the rule that federal funds be withheld from any state or local educational agency or institution which has the policy of preventing parents from inspecting, reviewing, and challenging the content of his or her child's school record. Outside access to these school records must be limited so that

protection of the student's right to privacy is ensured. It is recommended that the release of such identifiable personal data outside the school system be contingent upon the written consent of the parents or court order.

All persons, agencies, or organizations desiring access to the records of a student must complete a written form indicating the specific educational need for the information. This information shall be kept permanently with the file of the student for inspection by parents of students only and transferred to a third party only with written consent of the parents. Personal data should be made available for basic or applied research only when adequate safeguards have been established to protect the students' and families' rights of privacy.

Whenever a student has attained eighteen years of age, the permission or consent required of and the rights accorded to the parents should be conferred and passed to the student.

Finally, the Secretary of HEW should establish or designate an office and review board within HEW for the purpose of investigating, processing, reviewing, and adjudicating violations of the provisions set forth by the Congress.

JUVENILE RECORDS

The Task Force supports the basic philosophy underlying the existence of a separate court system for juvenile offenders, which is to avoid the stigmatizing effect of a criminal procedure. The lack of confidentiality of such proceedings and accompanying records subverts this intent and violates the individual's basic right of privacy.

Most states have enacted laws to provide confidentiality. Yet the Task Force finds that due to a lack of specific legislation, and contrary to the intent of the juvenile justice system, the individual's right of privacy is often routinely violated. Juvenile records are routinely released to the military, civil service, and often to private employers as well. This occurs in cases in which the hearing involves non-criminal charges, in cases of arrest but no court action, in cases in which the individual is no longer under the jurisdiction of the juvenile court, and in cases where his file has been administratively closed.

Legislation governing the confidentiality of juvenile court and police records varies widely from state to state. Only 24 states control and limit access to police records, therefore enabling a potential employer who is refused access to court records to obtain the information from the police. Only 16 states have expungment laws providing for the destruction of such records after a specified period of good behavior. Only 6 states make it a crime to improperly disclose juvenile record information. And, one state, Iowa, in fact provides that juvenile records must be open to the public for inspection. The Task Force finds that even in those states whose laws provide adequate protection, actual practices are often inconsistent with legislation.

Many new questions about confidentiality, privacy and juvenile rights are being raised, and the Task Force finds that the establishment of safeguards has lagged significantly behind technological developments. For example, presently no state has enacted legislation regulating the use of computers in juvenile court; as a rule, each sys-

tem establishes its own guidelines for data collection, retention, and distribution.

The Task Force finds that with the use of computers, the juvenile's right to privacy is additionally threatened by the increased accessibility to his record and therefore increased possibility of misuse. Staff carelessness, less than strict adherence to rules of limited access, and electronic sabotage must now be added to the existing threats to the juvenile's right to privacy.

The Task Force recommends the establishment of minimum federal standards for state laws to include the following provisions:

1. all records of the juvenile court and all police records concerning a juvenile shall be considered confidential and shall not be made public. Access to these records shall be limited to those officials directly connected with the child's treatment, welfare, and rehabilitation;

2. dissemination of juvenile records, or divulgence of that information for employment, licensing, or any other purpose in violation of statutory provisions shall be subject to a criminal penalty;

3. to protect the reformed delinquent from stigma continuing into his adult life, provisions should specify a procedure for either the total destruction or the sealing of all juvenile court and police investigative and offender records at the time the youth reaches his majority, or when two years have elapsed since he has been discharged from the custody or supervision of the court. Subsequent to this expungement, all proceedings and records should be treated as though they had never occurred and the youth should reply as such to any inquiry concerning his juvenile record; and

4. all police records on juveniles arrested but where no court action was taken should be systematically destroyed when the incident is no longer under active investigation.

The Task Force recommends the enactment of legislation specically prohibiting federal agencies from requesting information relating to juvenile record expnngement from employment applicants or from requesting such information from the courts or the police.

The Task Force further recommends the cessation of all federal funding for computerized systems which contain juvenile records unless it can be demonstrated that these systems provide adequate safeguards for the protection of the juvenile's right of privacy. These standards must fulfill all the requirements of the minimum standards for state legislation previously enumerated, including special provisions to strictly limit data accessibility.

ARREST RECORDS

A large percentage of arrests never result in conviction. Yet, in over half the states, individual's arrest records are open to public inspection, subjecting innocent parties to undue stigma, harassment, and discrimination.

Persons with arrest records often find it difficult, if not impossible to secure employment or licenses. A study of employment agencies in the New York City area found that seventy-five percent would not make a referral for any applicant with an arrest record. This was true even in cases in which the arrest was not followed by a trial and con-

viction. This is just one example of the widespread practice of "presumption of guilt" based on the existence of an arrest record.

The Task Force holds that release of information about arrests not followed by conviction is a direct violation of the individual's right of privacy. It therefore recommends that legislative efforts be directed toward:

1. establishing minimum standards, for state laws calling for the automatic sealing of all individual arrest records which were not followed by conviction and which are no longer under active investigation;

2. requiring the FBI to seal arrest records not followed by conviction; and

3. prohibiting inclusion of arrest records not followed by conviction on computerized systems involving more than one state or using federal funds.

MEDICAL RECORDS

Medical records, which contain sensitive and personal information, are especially in need of privacy safeguards to maintain basic trust in the doctor-patient relationship. Yet, development of automated data processing systems has enhanced the ability of government and private organizations to store, analyze and transfer medical records. Increasingly, this occurs without the individual's knowledge or consent. Abuse of such information systems can have a deleterious effect on doctor-patient relations.

To guarantee the privacy of medical records, the Task Force recommends that:

1. the Federal government provide dollar grants and incentives to States for the voluntary adoption and execution of State plans to insure the right to privacy for computerized medical information systems. Such a plan would place principal responsibility on the States, giving the federal government the right to set minimum standards;

2. Congress review the recently enacted Professional Standards Reviews Organizations (PSRO) legislation. There are increasing numbers of reports and complaints regarding Review Board uses of medical files and the threat this poses to privileged, confidential doctor-patient relationships; and

3. provisions be included in national health insurance legislation which specifically ensure the individual's privacy. The institution of a national health insurance plan will create a vast medical information network which will require stringent safeguards to prevent abuses of the patients' right to privacy.

COMPUTER DATA BANKS

The use of the computer has brought great commercial and social benefits to modern America. Greater reliance on the computer, however, increases its integration into all aspects of daily life. The result is increased vulnerability to abuse or misuse of computerized information.

The Task Force finds that the individual possesses inadequate remedies for the correction of such abuses. In fact, the Task Force

considers it probable that many abuses have gone unreported simply because the individual involved did not know of the data being collected about him.

Even if the individual is aware that data is being collected about him, he faces several obstacles if he wishes to expunge purely private information or to correct erroneous information. Among his obstacles are the following: the lack of statutory support for legal action (except in the credit reporting area), the cost of litigation, and even fear of retaliation by the company or agency being challenged.

Despite their potential for abuse, data banks remain an inescapable fact of life in a society growing more complex and more technological. The Task Force does not oppose data banks as such, but favors strong safeguards against their misuse, and recommends that:

1. Rights under the Fair Credit Reporting Act of 1970 be extended to all data collection. The individual must have and be informed of his right to review information contained in any collection of data about himself (excluding national security and criminal justice files);

2. Congress establish categories (i.e. indepth biographical, financial, medical, etc.) of information which may not be included in reports on an individual unless the individual knowingly gives his uncoerced consent;

3. limited exceptions be granted for national security and criminal justice investigations;

4. criminal and civil penalties be established for any use of statistical data (collected for collective analysis) to wrongfully acquire information on individuals;

5. transfer of personal information between governmental agencies be strictly limited;

6. the creation of a centralized Federal data bank (except for national security and criminal justice purposes) be prohibited; and

7. a federal "privacy protection agency" be established to enforce the proposed legislation.

CODE OF ETHICS AND STANDARD OF CONDUCT

The Republican Task Force on Privacy believes there to be a definite need for the development of a universal code of ethics and standard of conduct for the technical, managerial and academic personnel involved in the development and use of personal information systems. The Task Force regards this to be essential for the automated and computerized information systems. Personal information systems are becoming an integral aspect of the daily life of every individual in our society. This sensitive relationship demands and merits the development of an attitude of professionalism. It is recognized that some efforts have been made to develop and foster such attitudes. But, the information industry as a whole has not supported such efforts as a matter of policy. The Task Force declares its commitment to the development of a professional standard of conduct and code of ethics for the persons involved in the development, maintenance, management and use of personal information systems.

79-064 O - 76 - 15

CONCLUSION

The Task Force is aware that this is a relatively new area of concern. Some recommendations may go too far and some not far enough. Some areas may have been overlooked. But there is no question that now is the time to address ourselves to this important and far reaching issue. If we fail—George Orwell's 1984 may become a reality by 1976.

BIBLIOGRAPHY

Breckenridge, Adam Carlyle. *The right to privacy.* Lincoln, University of Nebraska Press, 1970.

Canada. Department of Communication and the Department of Justice. *Privacy and computers.* A report of a task force established jointly by the Canadian Department of Communication and the Department of Justice. Ottawa, Canada, Information Canada, 1972.

Campaigne, Howard and Lance J. Hoffman. Computer privacy and security. *Computers and automation*, v. 22, July 1973.

Cashman, Charles E. Confidentiality of juvenile court proceedings: A review. *Juvenile Justice*, v. 24, August 1973.

Cohen, Richard E. Justice report/hearings focus on privacy, limitations on use of FBI data. *National journal reports*, Feb. 16, 1974.

Computer applications in the juvenile justice system, National Council of Juvenile Court Judges, 1974.

Countryman, Vern. The diminishing right of privacy: The personal dossier and the computer. *Texas Law Review*, May 1971.

Curran, William J., *et al.* Protection of privacy and confidentiality. *Science*, v. 182, Nov. 23, 1973.

De Weese, J. Taylor. Giving the computer a conscience. *Harper's*, Nov. 1973.

Gotlieb, Calvin. Regulations for information systems. *Computers and automation*, v. 19, Sept. 1970.

Gough, Aidan A. The expungement of adjudication records. *Washington University Law Quarterly*, 1966.

Hunt, M. K. and Rein Turn. *Privacy and security in data bank systems; an annotated bibliography.* 1969–1973. R–1044–NSF. Santa Monica, Calif., Rand Corp., 1974.

Hoffman, Lance J. *Security and privacy in computer systems.* Los Angeles, Calif. 1973.

Hoglund and Kahan, Invasion of privacy and the freedom of information act; Geman v. NLRB, 40 *Geo Washington Law Review*, 1972.

Koehn, E. Hank. Privacy, our problem for tomorrow. *Journal of systems management*, v. 24, July 1973.

Kraning, Alan. Wanted: new ethics for new techniques. *Technology review*, v. 70, Mar. 1970.

Kuhn, David. Your life: how private? Reprint from *Minneapolis Tribune*, Oct. 7–12, 1973 by the Project on Privacy and Data Collection of the American Civil Liberties Union Foundation, Washington, D.C.

Lapidus, Edith J. *Eavesdropping on trial.* Rochelle Park, New Jersey, Hayden Book Co., 1974.

Levin, Eugene, The future shock of information networks, *Astronautics and aeronautics*, Nov. 1973.

Lusky Louis. Invasion of privacy : a clarification of concepts. *Columbia Law Review*, v. 72.

Miller, Arthur R. *The assault on privacy : computers, databanks, and dossiers.* Ann Arbor, University of Michigan Press, 1971.

Miller, Herbert S. *The closed door.* U.S. Dept of Labor, 1972.

National Committee for Citizens in Education. *Children, parents and school records.* Columbia, Md., National Committee for Citizens in Education, 1974.

Organisation for Economic Co-operation and Development. *Toward central government computer policies.* OECO Information Studies, 1973.

Pennock, J. Roland and John W. Chapman, *Privacy.* New York, Atherton Press, 1971.

Privacy in the First Amendment. *The Yale Law Journal*, June 1973.

Project Search Staff. Committee on Security and Privacy. *Security and Privacy considerations in criminal history information systems.* Technical Report No. 2. Sacramento, Calif., Project Search. California Crime Technological Research Foundation, July 1970.

Ralston, Anthony G. Computers and democracy, *Computers and automation*, v. 22. April 1973.

Reed, Irving S. *The application of information theory to privacy in data banks.* Santa Monica, Calif., Rand Corp., 1973.

banks. Santa Monica, Calif., Rand Corp., 1973.

Rul, James B. *Private lives and public surveillance.* London, Allen Lane, 1973.

Sargent, Francis W. Centralized data bank—where public technology can go wrong. *Astronautics and aeronautics*, v. 11, Nov. 1973.

Schrag, Peter. Dossier dictatorship. *Saturday Review*, April 17, 1971.

Social Security Administration. *Social Security Number Task Force : Report to the Commissioner.* Department of Health, Education and Welfare, 1971.

Springer, Eric W. *Automated medical records and the law.* Pittsburgh, Aspen Systems Corporation, 1971.

Stone, Michael and Malcolm Warner. *The data bank society : organizations, computers, and social freedom.* London, George Allen and Unwin LTD, 1970.

Thomas, Uwe. *Computerized data banks in public administration*, Paris, France, Organization for Economic Co-operation and Development, 1971.

Turn, Rein. *Privacy and security in personal information databank systems.* Prepared for the National Science Foundation. R–1044–NSF. March 1974. Santa Monica, Calif., Rand Corp., 1974.

U.S. Congress. House. Committee on Government Operations. *Federal information on systems and plans—Federal use and development of advanced technology.* Hearings before the Subcommittee on Foreign Operations and Government Information. 93rd Cong. 1st and 2d session, Washington, U.S. Govt. Printing Office, 1973, 1974.

U.S. Congress. Senate. Committee on the Judiciary. *Federal data banks, computers and the Bill of Rights.* Hearings before the Subcommittee on Constitutional Rights. 92nd Cong. 1st session, Washington, U.S. Govt. Printing Office, 1971.

U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems. *Records, computers, and the rights of citizens.* Washington, U.S. Govt. Printing Office, 1973.

Westin, Alan F. and Michael A. Baker. *Data banks in a free society; computers, recordkeeping, and privacy.* Report of the Project on Computer Databanks of the Computer Science and Engineering Board. National Academy of Science. New York, Quadrangle Books, 1972.

Wheeler, Stanton. *On record: files and dossiers in American life.* New York, Russell Sage Foundation, 1969.

QB1A

94th Congress
1st Session

COMMITTEE PRINT

SPACE BENEFITS—THE SECONDARY APPLICATION OF AEROSPACE TECHNOLOGY IN OTHER SECTORS OF THE ECONOMY

PREPARED FOR THE

COMMITTEE ON AERONAUTICAL AND SPACE SCIENCES UNITED STATES SENATE

APRIL 16, 1975

Printed for the use of the
Committee on Aeronautical and Space Sciences

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1975

45-713

J. LAW ENFORCEMENT

Key issue: *Computerized police information systems.*—The first real-time police computer system was installed in 1964 for the St. Louis department. In a 1971 survey of almost 500 police departments, 38.8% of the responding departments were using computers and 62.5% would be using computers by 1974. Applications include police patrol inquiries on wanted status of individuals or property ownership, automated traffic violation records, patrolman dispatching, automated files for criminal investigations, allocation and distribution of regular patrol units, and crime statistics. The Law Enforcement Assistance Administration (LEAA) has provided federal funds to police departments for computer acquisition. Police efficiency has been improved in some, but not all, instances. In addition, a controversy exists over cost effectiveness of computer use. (J–1).

[1] *J–1. Videotape storage and retrieval system.*—Computerized system developed for Marshall by Ampex Corp. (California) . . . NASA waived patent rights on key tape transport mechanism to Ampex in 1963 . . . improved and commercialized by Ampex as Videofile System . . . a single tape reel stores records from 10 four-drawer file cabinets, video output is of professional quality . . . total sales $23 million . . . most sales to law enforcement agencies, including Royal Canadian Mounted Police ($1.1 million system in 1971), Illinois Bureau of Criminal Investigations ($1.2 million, 1972), and Louisville Police Department (Kentucky, 1973) . . . provides *compact, automated fingerprint file system* used successfully in all installations and criminal history files (including photographs) in some installations . . . Canadian system will pay for itself in 3 years by reducing cost of fingerprint searches. (Contractor, TEF 226, Case No. 66201, 9/74).

J–2. Scientific and technical information management system (STIMS).—Developed for the Scientific and Technical Information Office, NASA Headquarters, as a computer software package for storing and retrieving bibliographic materials . . . obtained from STIF by the Law Enforcement Assistance Administration, Dept. of Justice (District of Columbia) . . . became the primary operating software for the National Criminal Justice Reference Service, a central computerized information system serving the nation's law enforcement and criminal justice agencies . . . NCJRS (became operational in September 1972) has 30,000 registered users and performed over 300,000 searches in 1973. (Personal contact, TEF 515, Case No. 103402, 9/74).

J–3. Systems analysis and computer modeling.—Developed for Headquarters by Jet Propulsion Laboratory (California) . . . used by JPL Public Safety Program, under contract to Los Angeles Police Department, for requirement definition and design of proposed city-wide emergency command and control communications system . . . includes master radio network plan, systems design for computer-

[1] Denotes transfer case related to key issue.

assisted dispatching, automated vehicle monitoring, automated mobile command center, automated precinct command center, out-of-car communications network, and detailed specifications for mobile digital communication system . . . will be first totally integrated system in country (cost to install over $50 million) . . . being established under LEAA funding as model program . . . consortium of major cities established to facilitate subsequent technology transfer. (Contractor, Contact/contractor, TEF 514, Case Nos. 103399, 103400, 9/74).

J–4. California four cities program.—Funded by NASA and NSF (since 1971) and managed by Jet Propulsion Laboratory (California) to transfer aerospace-generated technology to local governments . . . Aerojet-General Corp. providing Pasadena with a Science and Technology Advisor and technical support . . . Advisor used systems analysis to help Pasadena Police Department in selecting site for city heliport used by police helicopter, in compiling operations manual for effective helicopter patrol, and in developing program that reduced false alarms from burglary/robbery detection systems by 40%. (Contractor, TEF 512, Case No. 101915, 9/74).

Other relevant examples.—B–13 (OSHA noise regulations); D–1 (air pollution standards); E–2 (vehicle emission certification); E–4, E–9 and H–10 (implementing air quality laws); E–6 (legal evidence); E–7 (preparing environmental legislation); F–2 (OSHA safety regulations); G–5 (environmental lawsuit); I–5 (electrical code requirements).

92d Congress
1st Session

COMMITTEE PRINT

INVESTIGATION INTO ELECTRONIC BATTLEFIELD PROGRAM

REPORT

OF THE

ELECTRONIC BATTLEFIELD SUBCOMMITTEE

OF THE

PREPAREDNESS INVESTIGATING SUBCOMMITTEE

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE
NINETY-SECOND CONGRESS
FIRST SESSION

Printed for the use of the Committee on Armed Services

U.S. GOVERNMENT PRINTING OFFICE
56-743 WASHINGTON : 1971

LETTER OF TRANSMITTAL

U.S. Senate Electronic Battlefield Subcommittee
of the Preparedness Investigating Subcommittee,
Washington, D.C., February 22, 1971.

Hon. John C. Stennis,
Chairman, Committee on Armed Services, U.S. Senate,
Washington, D.C.

Dear Mr. Chairman: There is transmitted herewith a report of the Special Electronic Battlefield Subcommittee of the Preparedness Investigating Subcommittee appointed under Senate Resolution 331 of the second session of the 91st Congress.

This report sets forth the findings and conclusions of our inquiry into the electronic battlefield program. This term, as you know, is a loosely used phrase to describe many and varied types of surveillance equipment whose mission is to detect and locate enemy troops. The Subcommittee concentrated on the development and operational use of the most important types of new sensor surveillance equipment.

The testimony before the subcommittee conclusively demonstrated that sensors made a dramatic contribution toward saving a significant number of American lives in Southeast Asia.

It was a pleasure to serve as chairman of the Special Electronic Battlefield Subcommittee in response to your request.

Respectfully,

Howard W. Cannon,
Chairman, Electronic Battlefield Subcommittee.

I. INTRODUCTION

On October 18, 1970, a Special Electronic Battlefield Subcommittee of the Preparedness Investigating Subcommittee was established by Senator Stennis, chairman of the Senate Armed Services Committee.

Senator Stennis requested the special subcommittee to conduct a fact-finding investigation into what is commonly known as the electronic battlefield program. He requested the subcommittee to concentrate on the sensor surveillance systems, inasmuch as they are the most important parts of the overall program.

It was clear from the outset that the electronic battlefield program was not a clearly definable program as such. This term was used as the most readily available phrase to describe the many and varied types of equipment whose mission is to detect and locate enemy troops. One example will suffice to demonstrate this important point. Everyone is generally familiar with radars and the vital role they played during and subsequent to World War II. There are a wide range in types of radars to fulfill several different missions of detecting enemy ground forces, enemy aircraft, enemy ships, etc. If the subcommittee were to attempt to explore every radar system including its history and experience, it would have been necessary to conduct several weeks of hearings. This was not considered prudent or feasible.

Therefore, the subcommittee concentrated on the key area of interest, that is, the development and operational use of the new sensor surveillance equipment, as they were a vital new technology used for the first time to locate enemy forces in South Vietnam.

The use of sensors in Southeast Asia has been a somewhat confusing and misunderstood issue. This was quite natural because the program from the outset was shrouded in secrecy for obvious reasons. We did not want the enemy to know our plans, and we desired to take every possible precaution to protect the lives of our valiant soldiers in combat. Gradually, more and more information became available. Therefore, in keeping with the request of Chairman Stennis when he appointed the subcommittee, open sessions were held to the maximum extent possible in order to inform the American people concerning this important program. However, the subcommittee made it clear to all witnesses that it would not entertain testimony in open session that would jeopardize in any way the safety or security of our forces in Southeast Asia. Expert witnesses were heard from each of the military services.

This report sets forth the findings and conclusions of our investigation. The hearing record of the subcommittee contains a great deal of information about many sensors with photographs, performance characteristics, and so forth. In the interest of time and space, we have not reinserted that material in our report but respectfully refer the reader to the hearing record.

II. BACKGROUND

In August 1966, a scientific group known as the Jason Committee proposed to former Secretary of Defense McNamara a concept to impede enemy troop and supply infiltration into South Vietnam. An air supported barrier system and a conventional ground barrier system were to be established. This system called for the use of electronic sensors to detect enemy personnel and vehicles. Once enemy forces were detected, U.S. tactical aircraft, mines, and other munitions were to be called into action to prevent the enemy from successfully infiltrating into South Vietnam.

A special organization, the Defense Communications Planning Group, was established in September 1966 with responsibility to carry out the anti-infiltration systems conceived by the Jason Committee.

The conventional barrier system was called the McNamara Wall by the press. It combined sensors to detect enemy infiltration through the DMZ, physical obstacles to impede and canalize enemy movements, and tactical troop units operating from strong points, or fortified bases. While the original concept was never fully implemented, many types of sensor devices were placed in operation in Vietnam on an extremely high priority basis. The air supported system does not involve any ground forces. Sensors are air delivered along infiltration routes, their activations relayed via aircraft to a ground terminal for analysis and air strike recommendation.

The DCPG was given unprecedented authority. The Director was able to report directly to the Secretary of Defense, and thus achieve immediate decisionmaking action.

He was given responsibility for the entire program including design, development, test, requirements, procurement, and distribution. In effect, he was assigned control from "the cradle to the grave." In carrying out this mission, DCPG relied heavily on the military departments, JCS, and the SEA theater commander. DCPG tasked the military departments and outside agencies, particularly the Sandia Corp., to accomplish the necessary development and procurement invoking the highest industrial priority. It was provided ample funding to meet its mission objectives. As a result, major sensor systems were initiated immediately.

By the end of 1967 an initial anti-infiltration capability had been prepared and delivered to Southeast Asia within 15 months after the Secretary of Defense gave the go-ahead. This was the antivehicular subsystem of the air supported system.

The overall anti-infiltration system was designed to augment existing anti-infiltration efforts in SEA and to provide new capabilities for the interdiction program. A number of factors, i.e., political, military, terrain, and weather, dictated that the system take varied forms in different geographic areas. Thus, the initial capability was divided into two major systems: (a) DUEL BLADE, which was the conventional barrier system along the DMZ, and (b) IGLOO WHITE, the air supported system in Laos consisting of an antipersonnel and antivehicular subsystem. Anti-infiltration efforts in the mountainous area adjoining IGLOO WHITE and DUEL BLADE were to utilize assets of either system dependent on the tactical situation and the requirement.

The value of sensors was convincingly demonstrated during the battle at Khe Sanh where the resources intended for the antipersonnel

portion of the air supported system were diverted to meet the emergency. As a result, on April 5, 1968, the Defense Communications Planning Group was directed to procure sufficient sensor equipment necessary to support the incountry sensor program recommended by General Westmoreland. This program provided sensors for U.S. ground forces within South Vietnam rather than confining these devices to the anti-infiltration role. This program was nicknamed DUFFEL BAG.

* * * * * * *

XI. CONCLUSIONS

1. The unattended ground sensor surveillance system deployed operational for the first time in South Vietnam represented a great stride forward in the ability of our Armed Forces to detect and locate enemy forces.

2. The detection and location of enemy forces has been a formidable and challenging task since military forces historically took to the field for combat.

3. The sensors proved extremely valuable in ground combat as it enabled us to (*a*) deny the enemy his traditional cloaks of bad weather, jungle, and darkness; (*b*) surprise the enemy and cause him increased casualties and material damage; (*c*) locate the enemy with sufficient accuracy to permit effective engagement by artillery instead of troops on the ground; (*d*) prevent the enemy from disrupting our lines of communication through costly mining operations; (*e*) track the enemy movements in the so-called "rocket belts" around major cities and installations to preempt rocket attacks from taking the lives of our servicemen; and (*f*) significantly improve the security of U.S. installations.

4. The testimony conclusively proved that the sensors used in South Vietnam made a dramatic contribution in saving a substantial number of American lives and casualties.

5. The sensors used in South Vietnam were developed and produced in record time, and the subsequently improved sensor systems of longer operating life cost significantly less than the original sensor systems.

6. The sensor systems used by the Air Force were extremely valuable in locating truck convoys and were primarily responsible for establishing most of the targets in Laos.

7. There was $2.3 billion appropriated for this program, of which $678 million was returned to the services as not being required. This is probably one of the very few cases where moneys were ever returned as excess to the requirements of a given program. The subcommittee does not infer that "cost underruns" were experienced. However, in an era in which "cost overruns" seem to be the order of the day, it was refreshing to review a program where less money was spent than was originally anticipated.

8. The antipersonnel segment of the anti-infiltration system was never implemented. This led to the preparation of excessive requirements for some antipersonnel munitions. Some of these munitions were less capable than predicted; were hard to handle; and generally did not represent a productive investment of Government funds. The antipersonnel munitions purchased during the past 2 years have proven effective and appear to represent a worthwhile investment.

9. Antipersonnel munitions were never used in South Vietnam except in rare isolated instances. There is no record of injuries to U.S. personnel and only one reported instance of a Vietnamese noncombatant injury.

10. The Vietnamese Armed Forces have been effectively using sensors for some time and are enthusiastic about their application in a combat environment.

XII. RECOMMENDATIONS

The subcommittee recommends that:

1. The Army proceed cautiously on its integrated battlefield control system to insure that the planning is sound and that the tactical applications have been thoroughly explored before it requests significant funds of the Congress to implement the program.

2. Each military service, including the Defense Communications Planning Group, review on a continuing basis their respective sensor

devices to insure against any needless proliferation and that redundant systems be eliminated if they are found to exist.

3. The Department of Defense present in a concise manner and readily identifiable form all funds requested that are associated with surveillance programs so the Congress will have clear and precise information relative to the funds associated therewith. It is believed that the Department of Defense in the exercise of its judgment can achieve a better overall program definitization.

2. GENERAL ACCOUNTING OFFICE REPORTS

COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-171019

The Honorable Sam J. Ervin, Jr., Chairman
Subcommittee on Constitutional Rights
Committee on the Judiciary
United States Senate

Dear Mr. Chairman:

Your letter of February 21, 1974, requested that we provide your Subcommittee with information on the development and use of computerized criminal history information. You requested specific information in connection with hearings on legislation to guarantee the security and privacy of criminal history information (S. 2963 and S. 2964).

We have reviewed actions relating to the development of the Federal and State computerized criminal history information systems (CCH). Enclosed are our findings, which may be useful to your Subcommittee during its March hearings. We will provide the other information you requested after the hearings and further discussions with your staff.

Briefly, our findings indicate:

--When the Attorney General authorized the Federal Bureau of Investigation (FBI) to operate the CCH system in December 1970, he did not inform the FBI of (1) the extent to which certain criminal history information should have been maintained in Federal rather than State computers or (2) what type of advisory policy board should be established to review the policies and procedures used for CCH. He had, however, received recommendations regarding both matters from the Office of Management and Budget, Executive Office of the President.

--In the absence of such direction from the Attorney General, the FBI, with the concurrence of its National Crime Information Center Advisory Policy Board, developed the policy and operating procedures for CCH.

--There is some question as to the extent of computerized criminal history information which should be retained in the FBI's computers.

--Data is not available to indicate how computerized criminal history information has been used.

B-171019

--Both the FBI and the Law Enforcement Assistance Administration have either funded, or seek to develop, telecommunication system capabilities, to allow State and local criminal justice agencies to exchange administrative messages more effectively. The development of two systems could result in duplication and an unnecessary expenditure of Federal funds. Moreover, the Attorney General has not decided whether the FBI has legal authority to operate such a system.

The principal question which has resulted from our work to date, and which your Subcommittee might wish to pursue in its upcoming hearings, appears to be: What should the national policy be regarding development of computerized criminal history information systems, and to what extent should the various segments of the criminal justice community and appropriate Federal agencies participate in such policy development?

During the hearings the Subcommittee may wish to discuss with the Administration additional matters noted on pages 6, 8, and 10 of the enclosure.

We did not obtain comments from the Department on this report, but we did discuss the findings with cognizant officials, who generally agreed with the facts.

Sincerely yours,

Elmer B. Staats

Comptroller General
of the United States

Enclosure

79-064 O - 76 - 16

ENCLOSURE

DEVELOPMENT OF THE COMPUTERIZED CRIMINAL HISTORY INFORMATION SYSTEM

BACKGROUND

A cooperative effort of several States established and demonstrated the feasibility of using a computerized system for the interchange of criminal histories. The States' effort was called the System for Electronic Analysis and Retrieval of Criminal Histories (SEARCH).

The SEARCH project began receiving Federal funds in 1969 from the Law Enforcement Assistance Administration (LEAA) as part of LEAA's effort to encourage States to improve their criminal justice systems. SEARCH was developed on the basis that all computerized criminal history records would be stored in the States and that a central computer would maintain an index of abbreviated summary data on arrested individuals.

On request, a State was furnished this summary--which contained information on the reasons for and number of arrests and convictions--and, if necessary, could query the State listed on the summary as having the individual's records for the detailed information. LEAA gave the States about $4 million to develop and operate SEARCH.

SEARCH proved that it was feasible to use a computerized system for the interchange of criminal histories. The question then facing the Department of Justice was how to make the system operational: Who should operate the system? What computerized criminal history information should be contained at the Federal or at the State level?

The Attorney General's Office, the Federal Bureau of Investigation (FBI), and LEAA discussed the alternatives during the summer of 1970. One concern of LEAA was that the central index might contain too much detailed information, possibly raising the specter of a national computerized data bank. Regarding the extent of information to be contained in the central index, an August 1970 memorandum from the FBI Director to the Attorney General stated:

> "* * * no final decision has been made as to the exact details to be included in a national index criminal history record. This can only be done in coordination with the states. This Bureau plans no greater detail in the computerized criminal history record than is presently frequently available in the manually operated criminal identification record function."

Another issue was whether the FBI, LEAA, or the States should operate the system. The Assistant Attorney General for Administration supported the FBI's view that it was experienced in handling criminal information and should operate the system. LEAA basically proposed that it share operating responsibility with the FBI.

Before making any decisions the Attorney General requested the Office of Management and Budget (OMB) to study the alternatives for the future organization and operation of SEARCH. On September 3, 1970, the Associate Director of OMB recommended to the Attorney General that:

--The FBI operate the SEARCH central index on a limited record-length basis, while the States continue to develop and operate their individual, but compatible, automated criminal history systems.

--A strong Policy Control Board be established, which would report directly to the Attorney General, to decide the future development and operations of SEARCH. The Policy Control Board should include high-level officials from the FBI, LEAA, and the States, who should represent all elements of the criminal justice system (police, prosecutors, courts, corrections, and parole). Membership should be structured so that the States have an equal voice with the Federal Government in recommending policies for the future direction of SEARCH.

--Planning be initiated to develop an integrated criminal justice system. This would bring together SEARCH and the related FBI activities. The Policy Control Board should be the center of this planning activity.

On December 10, 1970, the Attorney General informed LEAA and the FBI that the FBI would take over management responsibility for a computerized criminal history system. However, we were told that the Attorney General did not follow or advise either LEAA or the FBI of OMB's other recommendations.

The FBI named the system the Computerized Criminal History (CCH) Program and operated it as part of its National Crime Information Center (NCIC), using NCIC computers and communication lines.

OPERATION

Since CCH is part of NCIC, a brief description of the system is useful.

Since the 1920's the FBI has maintained, in a manual central file in Washington, D.C., records of all arrests reported by local law

enforcement agencies and has disseminated such information, on request, to State and local law enforcement agencies. The arrests are reported to the FBI on fingerprint cards which are put in a file maintained for each arrested individual by fingerprint classification. Information from the fingerprint cards is transferred to a "rap sheet," making it a master list of all reported criminal activity for that particular individual. Disposition data is also supposed to be submitted by the arresting agency or the court on a disposition form and becomes part of the file maintained for each arrested person. Copies of the rap sheet are forwarded to local agencies in reply to requests for information on the particular individual.

The headings of information contained on rap sheets follow:

(1) contributor of fingerprints (usually arresting agency or correctional institution),

(2) individual's name,

(3) date arrested or received (i.e., sent to jail),

(4) nature of charge, and

(5) disposition.

The FBI began operating NCIC in 1967. Its current function is to supply, from a central data bank maintained by the FBI, an almost instantaneous response to inquiries from Federal, State, and local law enforcement agencies regarding fugitives; and stolen vehicles, license plates, securities, boats, guns, and other articles. Terminals at central State locations and at local law enforcement agencies are linked to a central computer, at FBI headquarters, which stores and disseminates this information on request. Other criminal justice agencies in the States can request NCIC information from these control terminals.

NCIC was developed with the assistance of an advisory group composed of State and local law enforcement personnel from agencies that either had computerized systems or were in the advanced planning stages of such systems.

The advisory group was replaced in 1969 by the NCIC Advisory Policy Board. The Board was composed primarily of State and local law enforcement personnel and made recommendations on NCIC policy to the FBI Director. Members were elected by the criminal justice agencies which had computer terminals linked to NCIC--mainly law enforcement, rather

than court or correction agencies. The Board obtains some input on how to operate the system from an annual meeting of users of the system.

Because CCH was an integral part of NCIC, the Board governing NCIC made recommendations to the FBI Director regarding CCH's development.

The NCIC Board, however, did not have as broad a composition as that of the board OMB envisioned when it made its September 1970 recommendations to the Attorney General; nor did it report directly to the Attorney General, as OMB had recommended.

In March 1971 the NCIC Board approved the operational concept, security requirements, and record content for the CCH program. The central data bank, as recommended by the Board and as agreed to by the FBI, would no longer merely point inquirers to the State where detailed criminal history information could be obtained. Instead, it would contain a detailed criminal history record on each offender whose record was entered by the States into the system. Basically, this detailed criminal history record would contain the information which the FBI had maintained manually on its offender rap sheets. It would consist of information showing the arresting agency, the reason and date of each arrest, and disposition and custody action, when available.

Maintaining the complete detailed record of each offender was to be an interim measure, according to the NCIC Board, because all users would not have the capability to fully participate in the beginning of the system. It would take time for the States to establish identification bureaus and develop fingerprint identification capability, information flow, and computer systems capability.

The ultimate concept of CCH, as envisioned by the Board, is a single-State, multi-State system. For single-State offenders NCIC would maintain only summary data and the States would maintain the detailed records. For multi-State offenders and for Federal offenders, NCIC would maintain the complete record. The summary record would include only the reason for arrests and number of arrests and convictions and specific information on the reason, date, and disposition of an offender's latest arrest and the criminal justice agencies involved. FBI studies have shown that about 70 percent of rearrests will be within the same State. Therefore, most detailed records will be for single-State offenders and ultimately maintained at the State level.

The NCIC Board in March 1971 had therefore committed itself to developing an operational system that went beyond the original SEARCH concept in terms of the Federal Government's involvement. The information in the FBI's computers would not be limited to abbreviated

summary data for single-State offenders, but would include complete criminal data on each offender until the States could develop fully operational CCH State systems. The FBI endorsed this concept, and the Board stated that the States should have fully operational systems by July 1, 1975.

State participation in CCH, in terms of entering records into the computer, is voluntary. But, any State which complies with the NCIC Board's security and confidentiality requirements can access information in the system.

Because the Attorney General did not follow all of OMB's recommendations, OMB officials held a meeting on April 26, 1971, with Department of Justice, LEAA, and FBI representatives to discuss CCH. Two of the major findings, according to a May 11, 1971, OMB memorandum of the meeting, were that:

--Neither the FBI nor LEAA had received copies of the September 1970 OMB report to the Attorney General.

--The FBI was building a central data bank of all criminal records instead of operating a central index as OMB recommended.

On May 13, 1971, the OMB Associate Director reported to the Attorney General that:

--The NCIC Board governing CCH had all police representatives instead of representatives from the total criminal justice system, including the courts, corrections, prosecutor, and parole segments, as OMB recommended.

--The NCIC computer system's policies limited CCH to police use. OMB intended that the system be used by the total criminal justice system.

--The rap sheets used in recording data included data on corrections and courts but those agencies did not have access to that data under the CCH system.

--Although authority existed for using statistical data from the system for criminal justice research, no firm commitments existed for making the data available for this purpose.

A September 1973 NCIC Board paper discussed the need for detailed information at the national level, noting that such information:

"* * * is required to efficiently and effectively coordinate the exchange of criminal history among State and Federal jurisdictions and to contend with interstate criminal mobility.

* * * * *

"* * * sufficient data must be stored in the national index to provide all users, particularly those users who do not have the capability to fully participate in the beginning system, the information necessary to meet basic criminal justice needs."

The same paper reiterated that for the system to be a truly national system the States must create fully operational systems by July 1, 1975.

Both FBI and LEAA officials, however, advised us that it is questionable whether many States can meet the July 1975 deadline. The probability exists that, because of the difficulty of developing systems in all the States, the FBI will retain detailed computerized criminal history information on single-State offenders for a substantial period.

In September 1973 the NCIC Board recommended that the FBI Director appoint some non-law-enforcement officials to its Board, since up to that time none of the Board members represented the court, prosecution, or correction segments of the criminal justice system. In February 1974 the Director appointed two prosecutors, two judges, and two correction officials to the Board. As of February 27, 1974, five had accepted the appointment.

Matter for consideration by the Subcommittee

The Subcommittee may wish to explore with the Attorney General whether he believes OMB's September 1970 recommendations are appropriate and, if so, how he intends to implement them.

USE OF CCH

On November 30, 1971, the CCH system became operational. As of February 17, 1974, six States and the District of Columbia, in addition to the Federal Government, had supplied computerized records to the system in the numbers shown below.

ENCLOSURE

Arizona	18,497
California	72,522
District of Columbia	45,099
Florida	70,480
Illinois	28,954
New York	46,285
Pennsylvania	10,177
United States Government[a]	156,487
Total	448,501

[a] Federal offenders are entered by the FBI.

This number represents only about 2 percent of the approximately 20 million individuals on whom the FBI has criminal history information. The CCH system, therefore, currently provides criminal justice agencies only a small portion of the total information they receive from the FBI.

Summary data the FBI gave us on the inquiries to CCH in January 1974 gives some indication of the type of requests coming to CCH. About 31,470 requests were received for either summary or complete CCH information. Of the approximately 25,900 requests for summary information, such as would be contained in the national index for single-State offenders, the CCH file contained information on 2,925, or about 11 percent. Of the approximately 5,570 requests for complete criminal history data to be transmitted back to the requestor by computers, the CCH file contained information on about 4,290, or 77 percent.

Data is not available at the national level to indicate for what purpose State and local criminal justice agencies use CCH information. The CCH system can identify the control agency terminals making inquiries to the system, but not the agencies within the State making requests of the control terminals. The States, however, would have such data. Moreover, there is no way to determine, from the computerized printouts, the purposes of inquiries.

An evaluation of SEARCH[1] attempted to determine police use of SEARCH, but the evaluation report noted that:

> "The observation of local police use of the system was not realized; therefore, this portion of the findings come from detailed interviews and not from operational experience. The most consistent opinion expressed by local police at all organizational levels is that criminal history is not vital prior to an arrest.

* * * * *

[1] The evaluation, completed on October 23, 1970, was done by Data Dynamics, Inc., Arlington, Virginia, for the California Crime Technological Research Foundation.

"The requirement is for a reliable source of accurate and timely information during the investigative phase, after an offender has been arrested."

The report, however, did not indicate the number of local police interviewed, their duties (such as patrol or identification), or whether those interviewed were randomly selected from all local police. Without such information, it is not possible to determine whether the views expressed to the evaluators are representative.

The SEARCH evaluation report did not address how court and correction agencies used computerized criminal history information, but noted that before SEARCH the "lack of criminal history data in the courts and correction functions was appalling."

Matter for consideration by the Subcommittee

We believe it is necessary to know what use is made of computerized criminal history information to determine what type of security and privacy provisions should be applied to the data and to provide management with sufficient information to determine how best to meet user needs. The Subcommittee may wish to discuss this matter with the Attorney General.

ADMINISTRATIVE MESSAGE SWITCHING

An important collateral development to the CCH system is the development of the communication system over which law enforcement agencies can exchange administrative messages on such matters as details of thefts of automobiles, or the transportation of arrested individuals.

The primary system used by the States is the National Law Enforcement Teletype System (NLETS). A consortium of States established NLETS in 1966 as a nonprofit corporation for the interjurisdictional exchange of criminal justice administrative messages. Teletype terminals in the States, accessible to local criminal justice agencies, interfaced with a central messageswitching terminal in Phoenix. NLETS was operated entirely on teletype equipment and had no data storage capability. The FBI was linked to the system with the same capabilities as the States. Each State financed its own participation in the network.

In 1973 LEAA and State and local law enforcement agencies became concerned that this low-speed system had become obsolete and could not meet the high-speed telecommunication needs of law enforcement agencies. Therefore, LEAA entered into an agreement with the National Aeronautics and Space Administration to have one of the Administration's contractors,

the Jet Propulsion Laboratory of the California Institute of Technology, develop alternatives for nationwide telecommunication systems to cover interstate criminal justice telecommunication needs up to 1983. The study will cost LEAA $500,000. The Jet Propulsion Laboratory is to issue its final report in mid-1974.

As an interim measure, LEAA gave the States $1.5 million in June 1973 to upgrade NLETS over a 42-month period so computers could be used to exchange information over high-speed communication lines. During the first 18 months NLETS was authorized to spend about $1.2 million to buy computer equipment, organize and install the high-speed communication lines, and bring in technical experts to implement the system. This upgrading, the initial phase of which was substantially completed in January 1974, enables computer-to-computer messages to be transmitted over the lines. As of January 31, 1974, about $741,000 had been spent.

Concurrently, the FBI expressed interest in operating law enforcement interstate administrative message switching. On July 11, 1973, the FBI Director requested the Attorney General's concurrence in his opinion that statutory authority for the FBI's NCIC included authority to provide expanded communications support for NCIC, including the switching of administrative messages and other interstate criminal justice communications. FBI officials advised us that the request to the Attorney General had been delayed until a permanent Director took office. Under the FBI's proposal, the FBI, rather than the States, would operate the central message switching unit to enable the different computerized information systems of the States to communicate directly.

The FBI pointed out that message switching is an integral part of the CCH system and that the NCIC communication network would be capable of handling all message switching requirements with minimal additional communication lines and upgrading of computer hardware.

According to an August 6, 1973, memorandum from the Department's Office of Legal Counsel to the Attorney General, it is arguable whether there is adequate legislative authority to support the FBI's proposal to acquire administrative message switching. Moreover, if the FBI obtains administrative message switching capability, there is a question whether NLETS needs to exist.

As of February 27, 1974, the Attorney General had made no decision on the FBI's request.

ENCLOSURE

Matters for consideration by the Subcommittee

Before moving forward with either LEAA's plans to continue upgrading NLETS or the FBI's proposal to implement administrative message switching, such Federal agencies as the Department of Justice, OMB, and the Office of Telecommunication Policy of the Executive Office of the President, should agree on what overall Federal involvement should be in computerized criminal justice telecommunication systems. The Subcommittee may wish to discuss these matters with the Attorney General.

REPORT TO THE HOUSE COMMITTEE ON THE JUDICIARY

BY THE COMPTROLLER GENERAL OF THE UNITED STATES

FBI Domestic Intelligence Operations--Their Purpose And Scope: Issues That Need To Be Resolved

The FBI's authority to carry out domestic intelligence investigations is unclear. Legislation is needed.

Investigations are too broad in terms of the number of people investigated and scope of investigations. Legislation is needed.

Investigations are generally passive in that information is gathered from other sources. But they are all encompassing. Questionable techniques were used infrequently, but legislation is needed limiting their future use.

The FBI adequately controlled dissemination of investigative information, but has not adequately examined its procedures for maintaining such data. The Attorney General should limit retention of investigative data.

Neither the Justice Department nor the Congress exercised adequate control and oversight over FBI domestic intelligence operations. Legislation is needed.

GGD-76-50

FEB. 24, 1976

COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-179296

The Honorable Peter W. Rodino, Jr.
Chairman, Committee on the Judiciary
House of Representatives

Dear Mr. Chairman:

This report, done in response to your June 3, 1974, request, describes how the Federal Bureau of Investigation (FBI) carries out its domestic intelligence operations and makes recommendations to the Congress and the Attorney General to improve such operations.

As you know, we made our review pursuant to the Budget and Accounting Act, 1921 (31 U.S.C. 53), the Accounting and Auditing Act of 1950 (31 U.S.C. 67), and the Legislative Reorganization Act of 1970 (31 U.S.C. 1156). Despite our clear authority in those acts to investigate the administration and operation of the FBI, the Attorney General denied us proper access to FBI investigative files. Thus, we cannot adequately assure the Committee and the Congress that our findings are complete.

Your June 3, 1974, letter mentioned that the Subcommittee on Civil and Constitutional Rights, chaired by Representative Don Edwards, would have responsibility for oversight of the FBI and requested that we work closely with the Subcommittee. Accordingly, we are also providing the Subcommittee copies of the report, and, as discussed with the Subcommittee, are providing copies to officials of the Department of Justice and the FBI. In addition, because of the extensive interest in the FBI's domestic intelligence operations, the Subcommittee agreed that the report should be provided to other appropriate congressional committees and Members of Congress, Government officials, and the general public.

We look forward to assisting your Committee in its continuing oversight of the FBI.

Sincerely yours,

Elmer B. Staats

Comptroller General
of the United States

COMPTROLLER GENERAL'S
REPORT TO THE HOUSE
COMMITTEE ON THE JUDICIARY

FBI DOMESTIC INTELLIGENCE OPERATIONS--THEIR PURPOSE AND SCOPE: ISSUES THAT NEED TO BE RESOLVED

Federal Bureau of Investigation
Department of Justice

D I G E S T

Changes are needed in the FBI's domestic intelligence operations. The operations are too broad in terms of the number of individuals investigated and the scope of the investigations.

Few would deny that some elements or groups within our Nation pose threats to our domestic security. But, differences appear on questions of the exact natures, intents, and threats of certain groups; the techniques used to identify and monitor them; and the scope of coverage applied to specific investigations.

It is a matter of deep concern to the security of our country and to the liberty of our citizens. Only through public debate, inherent in the legislative process, can the issues be adequately addressed.

GAO's recommendations are directed towards resolving problems in five main areas of concern:

--Authority for domestic intelligence operations.

--Initiating and continuing investigations and their results.

--Use of sources and techniques.

--Collection, dissemination, and retention of investigative information.

--Oversight and control.

The recommendations are based on GAO's analysis of 898 domestic intelligence cases randomly sampled from a universe of 19,659

cases acted on by the FBI during 1974 in 10 field offices.

AUTHORITY FOR DOMESTIC INTELLIGENCE OPERATIONS (Ch. 3)

Findings

The FBI appears to have carried out its domestic intelligence operations during the past 40 years within the broad framework of Presidential statements and directives, statutes, Executive orders, and Attorney General directives.

The FBI asserts that statements attributed to President Roosevelt in 1936 authorized and directed it to conduct intelligence investigations of subversive activities. But, alleged Presidential authorization is unclear as is the meaning of the term, subversive. What is clear is that in 1936 the FBI began intelligence investigations of the Communist and Fascist movements at the Secretary of State's request, pursuant to statutory authority in the FBI's appropriation act. Moreover, although the President had instigated the Secretary of State's request, the surrounding circumstances suggest that the President's concern was limited to organizations having some connection with a foreign government.

Subsequent Presidential directives in 1939, 1943, 1950, and 1953 did not explicitly delegate authority to the FBI to conduct intelligence investigations of subversive activities. To the extent, if any, that they fixed responsibility on the FBI for such investigations, they did not explicitly indicate that all types of domestic groups and individuals were subject to investigation or clearly indicate what constitutes subversive activities or subversion.

The FBI asserts parallel and preexisting statutory authority for domestic intelligence operations by contending that the

"detect and prosecute" language of 28 U.S.C. 533 authorizes intelligence investigations of groups and individuals who have violated or who are engaged in activities that may violate a substantive criminal statute, such as that pertaining to seditious conspiracy, 18 U.S.C. 2384. A precise definition of the duties intended to be encompassed by the phrase "detect and prosecute" is not possible because documentation related to congressional intent is either not available or does not provide an explanation. Therefore, the FBI's interpretation cannot be said to be incorrect.

Several directives from Attorneys General and other Justice Department officials, apparently issued pursuant to other provisions of 28 U.S.C. 533, also resulted in the FBI conducting certain domestic intelligence investigations. Additionally, Executive orders relating to the Security of Government Employees Programs have been cited as a basis of such investigations.

Conclusions

The FBI's authority to carry out domestic intelligence operations is unclear. It must be distilled through an interpretive process that leaves it vulnerable to continuous questioning and debate. There is a need for legislation that clearly provides such authority and delineates it in terms of objectives, scope, and functions encompassed.

Recommendations

GAO recommends that the Congress enact legislation concerning domestic intelligence operations clarifying the authority under which the FBI would be able to initiate and conduct such operations. In doing this, the Congress should (1) define the extent to which domestic intelligence investigations should be predicated on existing criminal statutes relating to the overthrow or advocating the overthrow of the Government and (2) specify the activities that should be investigated solely so appropriate Government officials can be aware of them.

Agency Comments

The FBI agreed that legislation is needed clarifying its authority to conduct domestic intelligence investigations. (See p. 163 and app. V.)

INITIATING AND CONTINUING INVESTIGATIONS AND THEIR RESULTS (Ch. 4, 5, 6, 7, 9, and 10)

Findings

FBI policy emphasizes that investigations are primarily made of groups and individuals whose actions may result in violations of criminal statutes, especially those dealing with rebellion or insurrection, seditious conspiracy, or advocating the overthrow of the Government. In practice, investigations of individuals occur because of their associations with groups the FBI has characterized as "subversive" or "extremist" regardless of whether the group is violent. (See pp. 27 to 42.)

The FBI primarily appears to justify domestic intelligence investigations on the need to provide the Attorney General and other officials with information upon which to make assessments and policy recommendations regarding the national security.

The FBI field office squad supervisor is responsible for day-to-day control of domestic intelligence investigations. He is responsible for insuring that (1) investigations are in accord with policy, (2) there is a sound basis for opening the investigation, and (3) results are achieved and reported to headquarters.

FBI officials stressed that investigative decisions are based upon the judgment of the agent. GAO believes decisions have to be made this way because the basis for such investigations is ambiguous and specific criteria delineating when to initiate them is lacking.

FBI officials stated that the rhetoric of a group or individual is sufficient to attract initial investigative interest if it could result in criminal violations and adversely affect the Nation's security.

Noticeable membership growth by a group advocating revolution would warrant an investigation as would such actions as buying and storing arms, engaging in firearms practice, or purchasing survival equipment.

Investigations can be initiated either at the preliminary or full-scale level, depending on the available facts and circumstances. The multilevel headquarters review of investigative decisions indicates the FBI's desire to strongly control field office investigations. What is lacking is an adequate independent assessment of the FBI's domestic intelligence policies and procedures.

The FBI believes its domestic intelligence programs fit within the policy framework for such investigations. GAO categorized the programs that came to its attention into five groups:

--Lists of individuals intensively investigated, which included the Security Index, the Communist-Reserve Index, the Administrative Index, and the Key Extremist and Key Activist Programs. (See pp. 66 to 75.)

--Special efforts to locate or follow certain individuals, which included the Stop Index, Computerized Telephone Number File, and the computerization of foreign travel effort. (See pp. 75 to 79.)

--Special liaison programs to focus attention on investigative problem areas, which included the False Identities Program and the efforts to be aware of extremist revolutionary, terrorist, and subversive activities in penal institutions. (See pp. 79 to 83.)

--Counterintelligence Programs. (See pp. 84 to 86.)

--Special reporting efforts of things such as civil disturbances and the "new left's" activities. (See pp. 86 to 90.)

Generally, the FBI's greatest consideration in developing such efforts has been the efficiency and effectiveness of them, rather than their

propriety in terms of protecting individuals' civil liberties. Although the FBI usually did not seek Justice Department approval for the programs, they largely coincided with Department interests.

GAO's review of the 797 randomly sampled cases on individuals showed that many investigations were opened on the basis of weak evidence concerning the nature and extent of the subjects' involvement with a subversive or extremist organization or activity and resulted in establishing either no or minor involvement by the subject.

GAO estimates, on the basis of its sample results, that about 32 percent of the 17,528 cases on individuals were initiated on the basis of hard evidence, about 32 percent on the basis of medium evidence, and about 36 percent on the basis of soft evidence.

--In the 263 sampled cases which the FBI initiated on the basis of hard evidence, it established that the subject was either a leader, member, or a violence prone person in 81 percent of the cases.

--In the 263 sampled cases initiated on the basis of medium evidence, the FBI established leadership, etc., in 49 percent.

--In the 271 sampled cases initiated on the basis of soft evidence, it established leadership, etc., in only 12 percent and found no association in 86 percent. (See pp. 99 to 103.)

Informants, the most common source of information, resulted in initiating 48 percent of the cases on individuals, compared to the next highest source, other FBI field offices, which provided such information in only 17 percent of the cases. (See pp. 103 to 106.)

State and local police, the principal outside sources used by the FBI to initiate investigations, were used in 12 percent of the cases. The remaining 23 percent of the cases were initiated on the basis of information received from confidential sources, other

Federal, State, or local agencies or from miscellaneous sources.

The strongest evidence by far was provided by the most common source of initiating information--FBI informants. Eighty-three percent of the cases initiated on the basis of such information were opened with either hard or medium evidence while only 17 percent were opened with soft evidence.

Overall, about 19 percent of the matters investigated by the FBI related to intelligence, domestic and foreign, from fiscal years 1965 through 1975. A further breakdown is classified because of the need to prevent disclosure of the FBI's counterespionage effort. But, the percentage has not varied greatly over the last decade, despite the increased emphasis given to domestic intelligence operations between fiscal years 1967-72. By fiscal year 1975, domestic intelligence operations had declined close to the 1965 level. (See pp. 131 to 137.)

FBI and Justice Department officials also estimate that the FBI spent about $82.5 million on general intelligence in fiscal year 1975. The estimated amount includes money spent on FBI staff involved in criminal as well as domestic and foreign intelligence operations but does not include all funds spent on certain technical support functions associated with such operations.

The purposes of the FBI's domestic intelligence investigations are to (1) prosecute and convict subjects for violating appropriate statutes, (2) continuously keep appraised of the strength, danger, and activities of subversive and extremist groups, and (3) provide information to assist executive branch officials in making decisions affecting national security.

There have been few tangible results from such investigations. This is not to say that domestic intelligence is unnecessary or of no value.

GAO estimated, on the basis of its random sample, that, of the 17,528 individual cases investigated by the 10 FBI field offices during 1974:

--3 percent (533) were referred for prosecution.

--1.6 percent (281) were prosecuted.

--1.3 percent (231) were convicted.

--2.7 percent (476) resulted in the FBI obtaining advance knowledge of planned activities. (See pp. 138 to 144.)

GAO also analyzed the 101 organization, or control and miscellaneous cases it sampled to determine whether any contained instances where the FBI obtained advance knowledge of planned activities. Twenty-one cases contained specific instances of advance knowledge. The number of instances in each case varied from 1 to 51. GAO considered 12 percent of such instances to be of a potentially violent nature. Others involved speeches, conferences, and demonstrations.

Furthermore, on the basis of its sample results, GAO estimates that:

--In 50 percent of 17,528 cases the FBI was unable to establish the individual's association with a group or its activities.

--In 44 percent (7,772), the FBI established that the individual was a leader, member of an organization, or violence prone individual. (See pp. 145 to 146.)

There was also a lack of evaluation and analysis capability in connection with the FBI's domestic intelligence operations. (See pp. 146 to 147.)

Other than effectively identifying and gathering information on groups and affiliated individuals that espouse and carry out subversive and extremist activities, the FBI's domestic intelligence operations do not appear to have achieved many tangible results. However, this may be sufficient, because who is

to say that the FBI's continuous coverage of such groups and their key leaders has not prevented them to date from achieving their ultimate subversive or extremist goals? The problem is one of adequately assessing the value and effectiveness of an operation which by its nature is preventive and by its mere existence may be accomplishing its purpose.

Conclusions

An essential difficulty with the domestic intelligence investigations has been the FBI's failure to adequately distinguish the extent to which groups are likely to use force or violence to achieve their goals and to investigate and use certain techniques accordingly. Priorities for such investigations are not systematically determined. Moreover, no outside organizations have effectively held the FBI accountable for such decisions.

Violent groups, such as the present-day Weatherman, or previously the Ku Klux Klan, warrant the FBI's full attention. Rather than concentrating on the most violence prone groups, the FBI has diffused its domestic intelligence investigative coverage to the point where many investigations do not lead to positive results. Perhaps if the FBI concentrated its efforts on those groups and individuals who represent the highest priority from a standpoint of a national security threat as determined by the Attorney General and FBI, the domestic intelligence program would be more productive.

GAO assumes that in any intelligence-type investigation, one objective must be to merely gather information. Such an objective is appropriate, but only within the confines of a clearly defined policy setting out the nature of groups and individuals to be investigated. Thus, the key decision must be that of deciding when to investigate a group or individual.

Recommendations

GAO recommends that the Congress enact legislation concerning domestic intelligence operations:

--Limiting such investigations only to groups that have used or are likely to use force or violence: a determination that must be made at least annually by the Attorney General or Deputy Attorney General in accordance with specific criteria issued by the Attorney General.

--Limiting investigations of individuals who are merely members of groups classified as warranting investigation, but which have only shown a likelihood of violence, to instances when information indicates the individuals may be involved in or are likely to become involved in specific criminal acts.

--Allowing the FBI to conduct yearlong, extensive investigations of individuals associated with, or suspected of associating with, groups that have proven abilities to commit violent acts and have been classified annually by the Attorney General or Deputy Attorney General as being grave threats to the public well-being. The phrase "proven ability to commit violent acts" could be defined by the frequency of acts and time period in which they were committed.

--Allowing the FBI to (1) establish and operate informants who could penetrate properly classified groups which have evidenced a likelihood of violence or used violence and (2) investigate leaders of such groups or potential groups to determine their identities, extent of their followings, and propensities for violence.

Agency Comments

The FBI did not agree that domestic intelligence operations should be directed only to those groups engaged in or likely to

engage in force or violence. The FBI essentially believes that it should be allowed to investigate groups that evidence a possibility of using violence, regardless of the probability that they will do so.

The Justice Department committee drafting FBI domestic intelligence guidelines stated in the guidelines that such investigations should be of activities which involve or will involve use of force or violence and the violation of Federal law.

The FBI also stated that GAO did not specifically address the need to investigate individuals unaffiliated with groups, which the FBI characterized as anarchists or terrorists.

No GAO recommendation would preclude the FBI from investigating any individual plotting the imminent use of force or violence in a specific criminal act. Moreover, GAO questions how the FBI presumes it could effectively obtain such knowledge of violent acts planned by individuals affiliated with no group when GAO results showed that the FBI obtained advance knowledge of actions--violent or otherwise--in few of the affiliated cases GAO sampled. (See pp. 163 to 165 and app. V.)

SOURCES AND TECHNIQUES (Ch. 7)

Findings

The FBI's domestic intelligence investigations are generally "passive" but all encompassing. Information is gathered from other sources, rather than being developed originally by the FBI.

The FBI first contacts a vast variety of routine, established sources to identify the subject and determine his or her activities. If those sources are unable to completely provide the required information, then the FBI uses interviews and other investigative

techniques. The use of special investigative techniques and programs seemed to depend on the results of the investigation. They were used once a subject's involvement in subversive or extremist activities was confirmed.

Informants and State and local police were by far the most common sources contacted during investigations. Informants were used in about 83 percent of the individual cases while police sources were contacted in about 77 percent. Confidential sources were used in 54 percent; credit bureaus, in 39 percent; educational institutions, in 21 percent; utilities, in 18 percent; and banks and other financial institutions, in 4 percent of the cases. (See pp. 106 to 108.)

With the exception of using certain minor investigative techniques to identify a subject, special or unusual techniques or programs were used infrequently. For example, the most common active investigative techniques used were pretext contacts and physical surveillance, which were both used in only about 20 percent of the cases. Photo surveillance was used in only 4 percent, while mail covers were used in only 1 percent of the cases. (See pp. 108 to 111.)

Interviews were conducted by the FBI in about 42 percent of the investigations of individuals. The subjects of the inquiries were interviewed in about 22 percent of the cases. Friends and associates were interviewed in 12 percent; neighbors, in 11 percent; employers, in 9 percent; relatives, in 9 percent; and others (including landlords, businessmen, attorneys and school officials), in 15 percent of the cases.

Information was obtained from electronic surveillances in only about 8 percent of all cases GAO sampled. In all but two of the cases, the information was obtained as the result of "overhears" on surveillances targeted against the subjects of cases not included in GAO's sample. Most electronic surveillances were targeted at the headquarters or chapters of subversive or extremist organizations. All were approved by the Attorney General.

There were only 6 cases in which the subjects were targets of neutralizing or disruptive actions under the FBI's counterintelligence programs. The actions consisted primarily of sending anonymous materials to the subjects and leaking nonpublic or disseminating public information to media sources. "Surreptitious entries" were used in nine sampled cases, and in one of those cases mail was opened. All but one of the cases were conducted by the FBI New York field office against groups or individuals classified as "subversive" by the FBI.

FBI policy has officially distinguished between preliminary inquiries and full-scale investigations since September 1973, to limit the impact of domestic intelligence investigations on the subjects and give headquarters greater control. Preliminary inquiries are to be undertaken through established sources, are not to exceed 90 days, and are to establish whether there is evidence to warrant a full-scale investigation. FBI field offices, however, did not distinguish between preliminary inquiries and full-scale investigations in practice.

GAO estimates that 7,562 of the 8,392 cases opened after December 31, 1973, were opened as preliminary inquiries. Moreover, the 10 FBI field offices generally used the same sources in preliminary inquiries as in full-scale investigations. Further, GAO estimates that inquiries lasted longer than 90 days in 72.5 percent of the cases and FBI headquarters was aware of such cases only about 35 percent of the time. Thus, many cases were not properly controlled. In December 1975 the FBI revised its policy to provide for better headquarters control of preliminary inquiries. (See pp. 111 to 116.)

Conclusions

Generally the FBI appeared to use appropriate techniques and sources during its investigations. Questionable actions were the use of counterintelligence techniques and surreptitious entry. Preliminary and full-scale

investigations, if properly implemented, could be an effective administrative aid and control. This concept, together with stricter, more specific requirements for opening investigations could help to limit the scope and conduct of the FBI's domestic intelligence operations.

Recommendations

GAO recommends that the Congress enact legislation concerning domestic intelligence operations limiting the extent to which the Attorney General may authorize the FBI to take nonviolent emergency measures to prevent the use of force or violence in violation of Federal law. Preventive measures should only be used when there is probable cause that violent actions pose real and immediate threats to life or property and would interfere substantially with the functioning of Government.

GAO recommends that, until guidelines or further legislative changes are enacted, the Attorney General direct the FBI to enforce its current requirements that (1) only established sources be contacted during preliminary inquiries and (2) preliminary inquiries be completed within the required 90-day time frame or that FBI headquarters approval be sought for an extension.

COLLECTION, DISSEMINATION, AND RETENTION OF INVESTIGATIVE INFORMATION (Ch. 8)

Findings

Overall, the FBI appears to have adequately controlled the dissemination of investigative information. However, the FBI had not adequately examined its procedures for maintaining information.

The FBI assumes that anything pertinent to an intelligence investigation will be included in a report and placed in a headquarters file. This information will be retained indefinitely because of the possibility that such data might be useful in future investigations. But,

neither the FBI nor the Justice Department has adequately determined the frequency and purposes of using investigative information after a case is closed. (See pp. 118 to 129.)

There was no indication that the collection of personal data was widespread. When it was recorded, agents generally indicated that it was unsolicited but included it in the file because it was provided by an informant or obtained through an electronic surveillance. (See pp. 120 to 121.)

There was some dissemination in 399--or about half--of the individual cases GAO sampled. Information was disseminated orally in only 6 percent of the cases, in writing in 79 percent, and both orally and written in 15 percent.

The U.S. Secret Service was the most frequent recipient of FBI-provided information--in 89 percent of the cases. But the Secret Service had intelligence files on the subjects of only about 4 percent of the cases GAO followed up with them. It destroyed the rest. Both FBI and Secret Service officials stressed the need to maintain the procedures governing the exchange of information between them, because it assures that there is little doubt that, if an individual investigated by the FBI meets Secret Service criteria, the Service would be aware of it.

Generally, the FBI appeared to adequately control the dissemination of information. But, improvements could be made. In 47 percent of the cases on individuals GAO sampled, the FBI could not establish any associations on the part of the subjects with subversive or extremist groups. Yet, in 21 percent of these cases the FBI disseminated reports identifying the individuals to other Federal, State, or local law enforcement agencies. Furthermore, in 71 percent of the cases opened in 1974 with dissemination, the dissemination was made during preliminary inquiries or during the preliminary stage of full-scale investigations.

Conclusions

GAO questions the need for disseminating information on individuals whom the FBI has not determined to be leaders, active members, or violence prone individuals because once the FBI disseminates information it loses control over how it is used, interpreted, and how long it is retained.

Recommendations

GAO recommends that the Attorney General direct the FBI to:

--Limit the type of information that can be collected by any source to that pertinent and necessary to the investigation.

--Establish a limit for the retention of all information obtained in domestic intelligence investigations after completing a study showing how, and the frequency with which, this information is used in subsequent investigations.

--Review, with appropriate agencies, current agreements regarding dissemination and exchange of information to assess the usefulness of FBI-provided information and if possible, reduce the amount of information exchanged.

--Only disseminate information relevant to an appropriate agency's organizational interest in the case, and in usual circumstances disseminate no information on individuals whose associations with a properly classified group or propensities for violence have not been established.

OVERSIGHT AND CONTROL (Ch. 5, 6, and 11)

Findings

Department of Justice officials exercised virtually no policy direction of FBI domestic intelligence investigations. In most instances when the Department requested particular investigations by the FBI, the request paralleled FBI efforts already underway.

Normally, Department of Justice policy guidance was provided only when the FBI requested it. However, the Department did not independently assess the extent to which the FBI was adhering to the guidance it did provide.

FBI investigations were not conducted in a vacuum. FBI internal documents frequently refer to the many inquiries from Government officials concerning the activities of individuals or groups. (See pp. 44 to 63.)

The Attorney General's draft guidelines for controlling domestic intelligence investigations are a step in the right direction and indicate a firm commitment to try to begin exercising proper departmental control of FBI operations. GAO believes the guidelines adequately address some of the problems associated with past and current domestic intelligence operations.

Under current FBI policy and the draft guidelines, preliminary inquiries are opened essentially to determine whether individuals associated with groups may be engaged in activities in which there is a likelihood that their actions will involve the use of violence. But, GAO found that many such inquiries did not result in positive information regarding the subject's association with a subversive or extremist group. There is a basis for questioning the need for such investigations. The draft guidelines do not adequately address the problem. (See pp. 148 to 157.)

Until recently, there has also not been any systematic or continuous congressional oversight of the FBI's domestic intelligence operations.

Conclusions

There must be continuous and conscientious oversight of domestic intelligence operations by the Justice Department and the Congress to help assure that the FBI's investigative efforts

are consistent with any legislative or administrative changes. Such decisions will, of necessity, be subjective to a certain extent, based on perceptions of domestic security at the time they have to be made. A broad spectrum of views should be marshaled in deciding the extent to which certain domestic intelligence efforts are needed.

Recommendations

GAO recommends that the Congress enact legislation requiring the Attorney General to periodically advise and report to the Congress on such matters as (1) the focus of current domestic intelligence operations, (2) groups under investigation, (3) anticipated actions of such groups and how they might affect policy decisions, and (4) the extent to which certain sensitive techniques, such as mail covers and preventive action, were approved and used.

GAO also recommends that the Attorney General publish specific rules and regulations establishing a systematic process for providing proper departmental control and oversight of FBI operations.

Some of these recommendations could be implemented by carrying out sections of the Attorney General's draft guidelines on FBI domestic intelligence operations. Others would require additional actions.

3. CONGRESSIONAL RESEARCH SERVICE REPORTS

U.S. Congress. Senate. Committee on Government Operations. Problems associated with computer technology in Federal programs and private industry: computer abuses. 94th Congress, 2d session. June 1976. pp. 153-165. (At head of title: committee print)

THE LIBRARY OF CONGRESS,
CONGRESSIONAL RESEARCH SERVICE,
Washington, D.C., June 11, 1976.

To Hon. Abraham Ribicoff, chairman, Senate Committee on Government Operations.
From: Louise Giovane Becker, analyst in information sciences.
Subj: Computer and information security in the Federal Government: An overview.

In response to your request for information on computer crime and security measures we have prepared a brief overview and selected articles on these matters for inclusion in the projected committee print. In addition, a bibliography has been compiled of relevant books, articles, monographs, and documents.

The overview examines some of the issues and activities related to protecting computers and data from possible misuse or abuse. Although the stress here is on computer security and computer-related crimes it should be understood that privacy and related issues are not to be totally ignored. The interrelationship of privacy concerns and computer security must be considered in the light of recent Federal agencies' activities.

The articles selected for inclusion reflect the overall concern and interest in this subject. Most of the references fall into two categories—computer security and computer-related crime. The intent of the compilation is to provide an understanding of the key issues. Many of the items reflect the concern of both the technologists and administrators in coming to grips with problems associated with the security of computers and automated information systems.

The cited references in the bibliography are divided into four major categories—computer security, criminal use of computer technology, bibliographies, and general/miscellaneous. The references selected should provide additional information and an understanding of the scope and nature of the related problems.

In recent years the necessity in both the private and public sectors to develop cohesive plans in the management of computers has become increasingly evident. The increase in computer crime and the possibility of intentional or accidental abuse that would compromise the computer operations have required additional safeguards. More effective management of computer and information resources will be the key to future developments.

I. INTRODUCTION

Computers and automated information systems are vulnerable to all of the security problems of manual information and recordkeeping operations as well as to a wide range of abuses and misuses unique to their special characteristics and conditions. Protecting information

79-064 O - 76 - 18

systems and their hardware requires an overall management concern and plan that includes the usual lock-and-key elements in addition to some special precautions.

Safeguards and security measures must be instituted that will protect the data processing facility, equipment (hardware), programs (software), data, and the integrity of the information. In other words, measures must include the protection of the entire operation. The level of protection must be in keeping with the data and operation to be protected and be consistently administered. The risk assessment must take into account the data and the scope and nature of the operation to be protected.

The focus of this memo will be primarily on overall Federal Government actions that reflect its interest in computer security and the prevention of computer crime. The activities of the intelligence community, while valuable to an understanding of computer security and risk assessment operations, will not be detailed in this discussion.

The extensive nature of the investment in and development of computer communication systems by the Federal Government is the major basis for instituting appropriate security measures. The Federal Government as the single largest user of computers, has well over 8,000 machines that provide a wide range of services and products essential to the welfare of the Nation. The handling, processing, and storage of data is key to many Federal programs and operations. Since computers and related technologies play a significant roll in the activities of a modern society it is essential that their utilization be properly controlled and managed. The misuse of these facilities, equipment, and data may have a serious impact on economic, political, and social activities of our citizens.

Some of the concepts and problems touched on here are presented in more detail a monograph by Peter S. Browne entitled "Computer Security—A Survey" which highlights some key technical problems and features an annotated bibliography.

Although some of the present activities regarding computer security stem from a concern for the privacy and protection of individual records, there has been consideration of the underlying issue—the management of information technology and resources. This focus is an essential and central issue in providing appropriate safeguards for computers and data handling operations. The cost of data processing operations and the importance to overall function of government agencies have placed special stress on the protection of information. Computer security has therefore become an essential and recognized aspect of managing information in the Federal Government.

DEFINITIONS FOR UNDERSTANDING

Computer security generally implies controlled access to both data and equipment. A few definitions are offered here to assist in providing an essential framework to understanding the issues and problems.

Security.—Is the protection of hardware, software, and data through the imposition of appropriate safeguards. Security comprises

data security, the protection of data against accidental or intentional destruction, disclosure or modification using both physical security measures and controlled accessibility, the set of technological measures of hardware and software available in a computer system for the protection of data.[1]

Data.—A general term used to denote any or all facts, numbers, that refer to or describe an object or ideas, condition, situation, or other factors. It connotes basic elements of information which can be processed or produced by computer.

On-line.—Direct access to a computer or data bank so that information is available instantly through a remote terminal device or computer console.

Time-sharing.—The utilization of computer or data banks by many individuals from remote terminal devices at the same time.

Physical Security.—The detail protection of computers and facilities against penetration, destruction, and disruption.

Data and Systems Security.—Examines the development of computer programs (software) and systems design to insure that the systems is protected.

Computer Crimes.—Usually includes theft, fraud, and embezzlement with the use of computers and related technology.

Definitions of additional terms are included in the attached glossary prepared by the National Bureau of Standards as part of the Federal Information Processing Standards program.

II. Background

Recent innovations and advances in technology have contributed to some of the problems of computer and information security. Computers permit efficient and economic storage, processing, and accessing of vast amounts of data. The development of large data bases with on-line (direct) access, has highlighted the need for better controls and safeguards. The increased use of remote terminals, video-screens, time-sharing, and browsing capabilities has stimulated the need to consider a re-assessment of access controls. In addition, the large dollar investment in both equipment and information has also encouraged the development of additional safeguards.

In less than three decades the computer has moved from the confines of the scientific laboratory to providing a wide range of services and products. It is generally recognized that computers are capable of handling diverse information problems—from complex space calculations to the design and ordering of parts; from manipulating simulation models to provide decisionmakers with alternatives to complex problems to assisting in issuing payments and invoices. The need to process vast amounts of data and the development of new computer applications have made Federal Government computer users increasingly dependent on this technology.

---

[1] Improving computer utilization. Computer technology at NBS. Dimensions, v. 57, Dec. 1973. p. 284.

As noted, most Federal Government programs and operations are highly dependent on the continued use of reliable computer and information systems. In recent years there has been a marked effort to develop appropriate safeguard guidelines which would optimize security in these systems. Computer security continues to be of concern to all elements of the Federal Government. In addition, the problem of protecting computerized information from criminal abuse has developed as an essential factor in the management of information handling systems.

Much of the initial interest and support for secure computers and systems has emanated from the military and intelligence communities. The sensitive nature of defense and national security information has fostered the development of secure systems in which planning and design carefully limit access. Sophisticated cryptologic (encoding devices), special hardware features, and unique software are employed to protect data and systems from unauthorized users. Many of the features of these security measures utilized by the defense and intelligence organizations have implications for the civilian sector as well.

A. GENERAL ACCOUNTING OFFICE REPORTS

Three reports issued by the Comptroller General's office, and included in this committee print, provide a review of some of the issues and problems related to computer security and crime. These reports focus on three significant problems in Federal systems—computer crimes, automated decisionmaking,[2] and the management of data processing facilities.

1. Computer Crimes in Federal Programs

The GAO report, "Computer-related Crimes in Federal Programs", highlights the potential vulnerability of Federal programs with regard to the use of "computer technology for fraudulent purposes". There is some difficulty in examining these problems due to the lack of adequate information. Federal agencies investigatory organizations often do not classify the crimes as such and therefore it is difficult to examine this problem. The report indicates that computer-related crimes coupled with an inappropriate use of computers have resulted in the need for Federal systems' managers to place more stringent controls on computer operations. The GAO recommends that specific measures be instituted to prevent criminal activities in computer systems. The report suggests that agencies undertake steps to prevent and discourage administrational and operational practices which might encourage computer crime activities.

A few articles have been included in the attached compilation that discuss the ways in which a computer served system can be penetrated and its data misused. Brandt Allen's article "Embezzler's Guide to the Computer" has been included in the compilation of articles because of its excellent survey of the vulnerabilities of computer systems.

---

[2] Automated decisionmaking describes specific applications that induce a set of actions without manual supervision or intervention.

2. Computerized "Automated Decisionmaking"

Many Federal agencies have installed computer applications that include inventory ordering and invoice/payment systems. The GAO report, "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government," examines some of the problems associated with automated decisionmaking and other associated problems of action directed computer programs. The GAO in reviewing some of these applications has called attention to the fact that poorly written programs and software often contribute to the difficulties. In addition, the study highlights the fact that unreviewed computer generated actions may cause the loss of billions of dollars in Federal Government assets.

3. Managing and Safeguarding Federal Facilities

The GAO report entitled "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities" discusses the security policies and practices that could ultimately deter and prevent losses in Federal Government data processing operations. The study recommends that the Office of Management and Budget (OMB) support administrative changes and provide additional guidelines in the area of physical security and risk assessment management.

B. FEDERAL AGENCIES' RESPONSIBILITIES

Due to recent disclosures regarding government surveillance and related activities there is a growing awareness of and concern with government recordkeeping responsibilities. In brief, government accountability regarding the management of information has been demanded. Although the Privacy Act of 1974 concentrates only on systems that contain personally identifiable data it has stimulated thought regarding the need to better regulate and administer all information systems.

Federal Government ADP (automatic data processing) management has been a shared responsibility among the Office of Management and Budget (OMB), General Services Administration (GSA), National Bureau of Standards (NBS), and the Office of Telecommunication Policy (OTP). In addition, individual departments' and agencies' data processing elements have contributed to developing management guidelines.

C. LEGISLATIVE REQUIREMENTS

Over the years there has been continued concern in Congress with the management of information and recordkeeping function in the Federal Government. Over the years the management of information and computers has been continuously monitored by individual Members of Congress and various congressional committees. In addition, legislation has been proposed and enacted to promote good management practices. Two laws have contributed directly to improving computer security measures in the Federal Government; Public Law 89–306 the "Brooks Bill' and P.L. 93–579, the Privacy Act of 1974.

1. P.L. 89–306 the "Brooks Bill"

The improvement of ADP management has been encouraged both through legislation and administrative actions within the Federal Government. The "Brooks bill" enacted October 30, 1965, provided "for the economic and effective purchase, lease, maintenance, operation, and utilization of automatic data processing equipment by Federal departments and agencies".

The law provides that OMB exercise fiscal control and provide policy guidance, GSA is to be responsible for ADP equipment procurement and maintenance functions, the National Bureau of Standards is authorized to provide technological advisory services and establish ADP standards.

2. P.L. 93–579, Privacy Act of 1974

In the 93rd Congress, the Privacy Act of 1974 was passed to "safeguard individual privacy from the misuse of Federal records." The law permits individuals access to records maintained by Federal agencies concerning themselves.

Under the Act the Office of Management and Budget was designated to "develop guidelines and regulations for the use of the agencies" and to provide continuing assistance in the implementation of the Act. As an initial step OMB drafted guidelines to provide agencies with an overall framework within which to delineate specific administrative procedures in keeping with the law. In addition, the General Service Administration and the National Bureau of Standards were tasked by OMB to provide specific guidelines.

Specific provisions of the Privacy Act that relate to computer security include:

limiting disclosure of personal information to authorized persons and agencies.

requiring accuracy, relevance, timeliness, and completeness of records, and

stipulating the use of safeguards to insure the confidentiality and security of records.

a. General Services Administration (GSA)

The GSA was requested to develop records management procedures to assist agencies in implementing the Privacy Act. These guidelines supplemented the OMB guidelines and regulations. The computer security requirements are to be evaluated prior to the procurement of new equipment or systems.

b. National Bureau of Standards (NBS)

NBS has concentrated on three categories of technical safeguards—physical security procedures, information management practices, and computer security/network controls. The Bureau has been active in encouraging the development of computer standards to improve the security and protection of automated data processing systems. Conferences have been held on computer security and risk assessment, cost and economic aspects related to security have been studied, and guidelines on computer security standards have been issued. Other aspects of standards development will be discussed below.

NBS is responsible for a series of documents that provide standards and guidance, some of which are cited in the attached list of selected references. The "Executive Guide to Computer Security", which is among the documents in the compilation, provides some direction to those responsible for the oversight and management of information systems.

III. Computer Security and Standards

The development of computer standards and related symbolic conventions has been encouraged by both private and public sector elements. Standards have permitted the full utilization of computer resources, more uniform and effective products, and have increased the range of communications. Government, as one of the largest users of computers, has worked with industry to provide guidelines and stimuli requisite to the development of standards' development. Recent legislation and the need to better manage information resources have stimulated the development of ADP standards.

The authorization for the development of a Federal ADP standards program came about with the passage of P.L. 89–306 (Brooks bill). The National Bureau of Standards has had a leadership role in assisting government and non-government users in the development, implementation, and maintenance of data standards through Federal Information Processing Standards (FIPS) task groups. These groups, composed of interdisciplinary teams from government, industry, and other concerned elements, have provided a set of voluntary national standards to improve computer and information systems performance.

A. FIPS 15 COMPUTER SECURITY

One of the task forces concentrating its efforts on providing standards for computer security is Federal Information Processing Task Force 15 (FIPS 15).

Although the activities of this group actually began before the passage of the privacy legislation, it has since focused on those security requirements outlined in the Office of Management and Budget "Privacy Act" (P.L. 93–579) "Implementation Guidelines" FIPS 15 has developed a taxonomy of computer security requirements, a glossary, and a security risk assessment paper.

Robert A. Courtney's paper "Security Risk Assessment in Electronic Data Processing Systems", prepared as a working document for FIPS 15, outlines some of the problems and issues in selecting appropriate data security measures. Detailed examination of the risk assessment process and the methodology are included.

Computer security improvement in the Federal Government is dependent in part on the development and implementation of standards and other activities. Certain initiatives have been taken by the NBS in examining selected approaches improving computer security. They have issued a number of documents of risk assessment and computer security. In addition, NBS has provided a forum for the discus-

sion of the new standards, cost-aspects of security and privacy, and has continued to provide assistance in some instances to other Federal agencies. (See Bibliography and compilation for other material.)

IV. Summary

As part of the overall concern for more effective and efficient use of modern technology computer security remains an important consideration. The possibility that computers can be used to perpetrate thefts and other criminal activity has provided an additional stimulus for improving risk assessment methods. Computer security is a necessary element in protecting data, software, equipment, and facilities from misuse. It is recognized that risk assessment activities and good management practices *must be combined* to provide maximum protection of the facility and its information.

The compilation of materials and references included in the committee print are intended to provide an initial framework for understanding the scope and nature of this complex problem. Federal Government must be responsive so that maximum protection is obtained at a reasonable cost. Safeguards and guidelines must also reflect the intent of existing legislation and congressional concern.

In reviewing ADP management practices, some important issues emerge that require additional consideration by Congress and other responsible Federal government elements.

One of the problems to be confronted is the call for total evaluation of ADP management practices in the Federal Government. Interested observers have often pointed to the lack of coordination and communication among Federal departments and agencies in planning and administering computer and information systems. There are indications that a more integrated approach to managing information systems may help to ensure that both economic and social factors are considered in the development of new systems.

Further investigation, undertaken in light of recent disclosures discussed in the GAO reports, might be required. The recommendations outlined in the reports and suggestions from other investigations must be considered. Some key issues have been identified that require further consideration by all responsible elements in Federal Government:

Should ADP management in the Federal Government be better organized and strengthened to ensure better use of resources?

Is there need for an indepth assessment of security and related concerns in the Federal Government?

Should further research be instituted on developing better performance measurements?

The re-evaluation of ADP management practices must occur within the context of expanded national information needs and the rapid emergencies of important innovations in technology. In the next few years Congress will consider programs such as national health care that will make unusual demands of our information handling practices. Therefore it becomes essential to have secure and well protected systems. In addition, as new services are initiated and old ones expanded, there will be a need for better government information support. This support must place special requirements on computer secu-

rity elements to ensure the integrity of the system and to prevent computer abuse by those with criminal intent.

JK 1015C 76-54 G

CONGRESSIONAL OVERSIGHT OF INTELLIGENCE: STATUS AND RECOMMENDATIONS

FREDERICK M. KAISER
Analyst in American National Government
Government Division

March 11, 1976

CONGRESSIONAL RESEARCH SERVICE
LIBRARY OF CONGRESS

Contents

	Page
Introduction...	1
I. Current oversight of intelligence...	2
A. Oversight in general...	2
B. Intelligence agencies, foreign and domestic...	3
C. Dispersal of intelligence oversight...	5
D. Evaluations of intelligence oversight...	9
II. Intelligence oversight authority and restrictions...	10
A. Mandate...	11
B. Jurisdiction...	13
C. Staff and support services...	13
D. Subpoena/contempt powers...	21
E. Immunity for witnesses...	26
F. Disclosure of information and materials...	27
III. Reorganization proposals relating to intelligence oversight...	32
A. Government commissions...	33
1. Commission on the Organization of the Executive Branch of the Government, 1953-55 (2d Hoover Commission)...	33
2. President's Commission on CIA Activities Within the United States (Rockefeller Commission)...	35
3. Commission on the Organization of the Government for the Conduct of Foreign Policy (Murphy Commission)...	36
B. Congressional recommendations, historical review...	39
1. S. Con. Res. 2 (1955-56)...	40
2. S. Res. 283 (1966)...	41
C. Current congressional recommendations...	42
IV. Bibliography...	49

CONGRESSIONAL OVERSIGHT OF INTELLIGENCE: STATUS AND RECOMMENDATIONS

> If men were angels, no Government would be necessary. If angels were to govern men, neither external nor internal controls on Government would be necessary. In framing a Government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place, oblige it to control itself.
>
> James Madison, Federalist #51 1/

While James Madison alludes in the above passage to the function of congressional oversight and its importance in democratic government, Woodrow Wilson, writing in Congressional Government, is even more emphatic: "Quite as important as legislation is vigilant oversight of administration."2/ Ideally, legislative oversight of the Executive serves numerous purposes -- to guarantee administrative compliance with legislative intent; to control wasteful, excessive expenditures; to promote efficient operation; to assure proper accounting of expenditures; to discover malfeasance in office and curtail arbitrary and abusive exercise of bureaucratic authority; and to guarantee compliance with constitutional dictates. In essence, legislative oversight of the bureaucracy is to ensure the accountability of non-elected administrators to the elected representatives of the public.

1/ Alexander Hamilton, James Madison, and John Jay, The Federalist Papers (New York: The New American Library edition, 1961), p. 322. Among the 85 Federalist Papers, the series of papers published under the pseudonym of Publius in support of ratification of the Constitution, Federalist #10 and #51, both contributions of Madison, are regarded as the most important because of their defense of the principles of checks and balances and the separation of powers.

2/ Woodrow Wilson, Congressional Government (Boston: Houghton Mifflin, 1900, 15th edition), p. 297. Wilson, whose analysis was initially written in 1885, was not sanguine, however, about the effectiveness of congressional oversight. He wrote...

> It is quite evident that the means which Congress has of controlling the departments and of exercising the searching oversight at which it aims are limited and defective. (p. 270)

The general mandates for congressional oversight have been reflected in the congressional reorganization efforts of the post-WW II era and most recently in relation to the United States intelligence agencies. The select committees on intelligence of the 94th Congress in the House and the Senate 3/ and proposals to create permanent standing committees on intelligence are part of long-term and recurrent tendencies in the congressional process -- to emphasize oversight and to restructure oversight of intelligence agencies and activities. This report examines the current oversight efforts in the Congress, including the select committees; oversight authorities and restrictions on comprehensive oversight of intelligence; and reorganization proposals relating to intelligence oversight, including the recommendations of Federal government commissions and the Congress.

I. Current Oversight of Intelligence

Oversight in general has been a prominent concern of Congress in the post-WW II era, despite some analysts' view that it is "Congress' neglected function."4/ The 1946 Legislative Reorganization Act (P.L. 79-601)

3/ The House Select Committee on Intelligence was established by H. Res. 138 on Feb. 19, 1975 and replaced by an expanded select committee possessing identical authority and mandate by H. Res. 591 on July 17, 1975. The Senate Select Committee to Study Government Operations with Respect to Intelligence Activities was created by S. Res. 21 on Jan. 27, 1975.

4/ John Bibby, "Oversight: Congress' Neglected Function," in Melvin Laird (ed.), Republican Papers (New York: Praeger Publishers, 1968). Other sources include John Bibby, "Committee Characteristics and Legislative Oversight of Administration," Midwest Journal of Political Science, vol. 10 (1966); Cornelius Cotter, "Legislative Oversight," in Alfred de Grazia (ed.), Congress, the First Branch of Government (Garden City, New York: Doubleday and Co., 1967); William Morrow, "Congressional Control of Administration Discretion," Journal of Politics, vol. 30 (1968); Thomas Jahnige, "The Congressional Committee System and Oversight: Congress and NASA," Western Political Quarterly, June, 1968; Joseph Harris, Congressional Control of Administration (Garden City, New York: Anchor Books, 1965); Thomas Henderson, Congres-

and its 1970 counterpart (P. L. 91-510) are the major pieces of legislation regarding oversight. Sec. 136 of the 1946 act mandated "continuous watchfulness" over the executive and Sec. 118 of the 1970 statute provided dual requirements for legislative review--" each committee shall review and study, on a continuing basis, the application, administration, and execution of laws" under its jurisdiction and report those activities to the full chamber at the end of each Congress. On Oct. 8, 1974, the House of Representatives adopted H. Res. 988, the Committee Reform Amendments, which provided for shared oversight jurisdiction through special oversight functions. Special oversight permits a committee to conduct oversight of specific subject matter which is not under its legislative jurisdiction but which relates to its responsibilities. In the case of intelligence, the House Committee on International Relations was granted special oversight of intelligence activities relating to foreign policy, formerly the exclusive province of the Armed Services Panel.

Oversight of intelligence is widely dispersed among congressional committies, especially when considering foreign as well as domestic intelligence agencies. The following lists the relevant agencies which have been designated as foreign or domestic intelligence agencies.

---

sional Oversight of Executive Agencies (Gainesville, Fla.: University of Florida Press, 1970); Morris Ogul, "Legislative Oversight of Bureaucracy" and Walter Oleszek, "Congressional Oversight: Methods and Reform Proposals," published by House Select Committee on Committees, Committee Organization in the House, Panel Discussions, vol. 2, part 3, pp. 692-724 (Washington, D. C.:U. S. Govt. Print. Off., 1973).

Foreign Intelligence Agencies[a]

Central Intelligence Agency (CIA)

Defense Intelligence Agency (DIA)

Department of State--Bureau of Intelligence and Research

Department of the Treasury--Office of National Security

Energy Research and Development Administration (ERDA) (formerly Atomic Energy Commission (AEC))

National Security Agency (NSA)

United States Air Force--Assistant Chief of Staff, Intelligence

United States Army G-2, Assistant Chief of Staff, Intelligence

United States Navy--Naval Intelligence Command

United States Navy--Marine Corps G-2

[a] Foreign intelligence agencies may be regarded as those affiliated with the United States Intelligence Board (USIB), the interdepartmental body which coordinates foreign intelligence activities. The Director of Central Intelligence chairs USIB, which was created by a National Security Council Directive. All the agencies listed as foreign intelligence agencies are members of USIB except for the intelligence units of the principal military departments, which serve as observers, and the Marine Corps, which has no direct representation or observer status but which has an intelligence component.

Domestic Intelligence Agencies[a]

Civil Service Commission	--Bureau of Personnel Investigations
Department of Defense	--Defense Investigative Service
Department of Justice	--Criminal Division[b]
	--Drug Enforcement Administration (DE
	--Federal Bureau of Investigation (FBI)
	--Immigration and Naturalization Servi

Department of State	--Passport Office, Bureau of Security and Consular Affairs
Department of Transportation	--U.S. Coast Guard
Department of Treasury	--Bureau of Alcohol, Tobacco, and Firearms
	--Internal Revenue Service
	--Secret Service
	--U.S. Customs Service
U.S. Postal Service	--Inspection Service (formerly Intelligence Division)

[a] Domestic intelligence agencies are more difficult to designate than their foreign counterparts because of the absence of an interdepartmental coordinating device similar to USIB. Although there is a lack of consensus among researchers and practitioners regarding domestic intelligence (vis-a-vis foreign intelligence), this chart lists agencies which have reportedly engaged in domestic intelligence production.

[b] In 1954 the Internal Security Division was created within the Justice Department in addition to the existing Criminal Division, but was abolished in 1973 and its powers, functions, and duties were transferred to the Criminal Division.

The diversity of the United States intelligence community suggests that its oversight will be correspondingly dispersed among numerous congressional committees. In addition to the Appropriations Committees which have oversight authority over the agencies by virtue of the appropriations process, the committees which have exercised oversight include Armed Services, Government Operations, Foreign Relations and International Relations, Judiciary, Post Office and Civil Service, and Ways and Means and Finance. The Joint Committee on Atomic Energy (JCAE) and

Joint Committee on Internal Revenue Taxation (JCIRT) also have conducted oversight regarding intelligence agencies and/or activities of AEC/ERDA and the IRS, 5/ respectively. Most recently, the House and Senate select committees on intelligence have functioned as oversight/investigative units with regard to a broad spectrum of domestic and foreign intelligence agencies and activities. Both select committees possessed comprehensive jurisdictions. S. Res. 21, approved Jan. 27, 1975, empowered the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities to conduct an investigation and study regarding illegal, improper, or unethical activities "engaged in by any agency or by any persons acting either individually or in combination with others, in carrying out any intelligence or surveillance activities by or on behalf of any agency of the Federal Government." (emphasis added) H. Res. 138, approved on Feb. 19, 1975, authorized the House Select Committee on Intelligence "to conduct and inquiry into the organization, operations, and oversight of the intelligence community of the United States Government" and, after listing certain specific agencies as objects of the inquiry, included "any other instrumentalities of the United States Government engaged in or otherwise responsible for intelligence operations in the United States and abroad." (emphasis added)

5/ An example of JCIRT oversight activity is a report by its staff, empowered by the Committee" to investigate charges that the Nixon Administration used the Internal Revenue Service... for partisan political purposes," which focused on the Special Service Staff, an internal IRS unit created in 1969 (and terminated in 1973) to gather information on "extremist" organizations. Joint Committee on Internal Revenue Taxation, Investigation of the Special Service Staff of the Internal Revenue Service (prepared for the Joint Committee by its staff, June 5, 1975) (Washington: U.S. Govt. Print. Off., 1975), p. III.

Oversight of intelligence agencies and activities may occur as a by-product of other congressional responsibilities, such as appropriations, authorizations, and legislation for executive agencies under a committee jurisdiction, as mandated by the Legislative Reorganization Acts of 1946 and 1970; may be expressly delegated to a committee (e.g., special oversight jurisdiction and mandate of the House Committee on International Relations, oversight of ERDA by JCAE); may occur as a by-product of an investigation of related subject matter (e.g. protection of constitutional rights6/) or of a special investigation by a select committee, as with the House and Senate select committees on intelligence or the Senate Select Committee on Presidential Campaign Activities (Watergate Committee); or may be part of the broad mandate, relating to the economy and efficiency of Government operations and activities and reorganizations of the executive branch, which the Committees on Government Operations hold.

A recent piece of legislation which augments the intelligence oversight jurisdiction of the House Committee on Internal Relations, Senate Foreign Relations, and other appropriate committees, is the Foreign Assistance Act of 1974 (P.L. 93-559 ; 88 Stat. 1795). Sec. 32 of the 1974 Act amended Sec. 662 of the Foreign Assistance Act of 1961 to provide the following reporting requirements regarding certain CIA foreign operations:

> Sec. 32. The Foreign Assistance Act of 1961 is amended by adding at the end of part III the following new sections:

6/ For example, see the investigations sponsored by the Senate Subcommittee on Constitutional Rights, inquiring the history, origin, and activities of the Special Service Staff of the Internal Revenue Service and into domestic military surveillance of civilians.

"Sec. 662. Limitation on Intelligence Activities. --(a) No funds appropriated under the authority of this or any other Act may be expended by or on behalf of the Central Intelligence Agency for operations in foreign countries, other than activities intended solely for obtaining necessary intelligence, unless and until the President finds that each such operation is important to the national security of the United States and reports, in a timely fashion, a description and scope of such operation to the appropriate committees of the Congress, including the Committee on Foreign Relations of the United States Senate and the Committee on Foreign Affairs of the United States House of Representative.

"(b) The provisions of subsection (a) of this section shall not apply during military operations initiated by the United States under a declaration of war approved by the Congress or an exercise of powers by the President under the War Powers Resolution."

It should be noted that this legislation is comprehensive regarding CIA operations abroad of a non-intelligence nature. The provision applies to activities financed by Foreign Assistance Act funds, those financed by transfers from other accounts, and those supported by covert funds made available through Department of Defense authorizations. 7/ The limitation is technically only a reporting requirement and does not include provision for a congressional or committee veto. 8/ The appropriate committees, in other words, cannot prevent or halt any particular operation or activity

7/ For an elaboration of spending powers by the CIA, see Louis Fisher, Presidential Spending Power (Princeton, N.J.: Princeton University Press, 1975, pp. 214-221 and Anon., "The CIA's Secret Funding and the Constitution," Yale Law Journal, vol. 84, no. 3 (Jan. 1975).

8/ The legislative, congressional, or committee veto, terms often used interchangeably, usually provides that specific administrative actions shall not be implemented until an appropriate committee or the Congress reviews and approves or does not disapprove (veto) the action. A specific time period is provided in such legislation. An example of the congressional veto is found in the Executive Reorganization Act, codified in title 5 of the United States Code, sections 901-913 (1970). The reporting requirement contained in the 1974 Foreign Assistance Act only directs the President to report certain operations and does not provide a congressional mechanism for vetoing or disapproving any actions. Although notice provisions are not as dramatic as veto provisions, the former can have an immediate and direct impact on Executive actions through the congressional review process and implicit advisory position of the committees. Further discussion of the congressional veto is presented in a later section.

on the basis of this legislation. Furthermore, there is no requirement that the description and scope of the activity include estimated expenditures or manpower committed. Finally, the reporting requirement is suspended in cases of a formal declaration of war or an exercise of powers by the President under the War Powers Resolution.

During the past quarter century, the formal changes affecting congressional oversight of intelligence have been the creation of the select committees on intelligence, the addition of the special oversight function regarding CIA foreign operations delegated to the House Committee on International Relations, and the procedural reporting requirements included in the 1974 Foreign Assistance Act.

Intelligence oversight has received mixed reviews throughout this time period. In 1950 Robert Dahl wrote...

> To improve the legislative position in foreign affairs vis-a-vis the executive, one means is a better relationship between the Congress and the CIA; indeed, almost any relationship at all might constitute an improvement over the present hiatus. 9/

Current critics of congressional oversight of the intelligence community are not as harsh, although they point to the continued absence of comprehensive oversight due to the dispersal of jurisdiction and to the restrictions on congressional oversight. Harry Howe Ransom recently evaluated the state of oversight as follows:

> The argument is not that congressional attention to the intelligence system has been absent. But such attention has been sporadic, unsystematic, incomplete, and at times casual... If this is so, Congress is susceptible to manipulation by the executive branch. 10/

9/ Robert Dahl, Congress and Foreign Policy (New York: Harcourt Brace and Co., 1950), p. 155. Dahl, a former president of the American Political Sciences Association, is professor of political science at Yale University.

10/ Harry Howe Ransom, "Congress and the Intelligence Agencies," in Harvey C. Mansfield (ed.), Congress Against the President, Proceedings of the Academy of Political Science, vol. 32, no. 1, (1975) p. 159.

Defenders of the existing state of congressional oversight respond to such observations by referring to the extensive oversight responsibilities among numerous committees and subcommittees, the ability of the Congress to react, when necessary, to accusations through specialized, ad hoc investigative units, such as the Watergate Committee and the select committees on intelligence, and the frequent briefings and reports presented by intelligence officials to the Congress.

II. Intelligence Oversight Authorities and Restrictions

With regard to oversight in general, the House Select Committee on Committees concluded in its final report in 1974 that "Representatives and other witnesses were virtually unanimous in acknowledging the inadequate oversight being done by congressional committees."11/ Roger Davidson, formerly a professional staff member of that Select Committee, described oversight as "one of Congress' most glaring deficiencies."12/

Ransom, the author of several works on the intelligence community, including The Intelligence Establishment (Cambridge, Mass. Harvard University Press, 1970), is a professor of political science at Vanderbilt University.

11/ House Select Committee on Committees, Committee Reform Amendments of 1974, Report, 93d Congress, 2d session (Washington, D.C.: U.S. Govt. Print. Off., 1974), pp. 62-63.

12/ Roger Davidson, "Representation and Congressional Committees," in Annals of the American Academy of Political and Social Science, vol. 411 (Jan. 1974). This volume of the Annals is entitled Changing Congress: The Committee System and edited by Norman Ornstein.

These characterizations of inadequate, unsystematic, and uncomprehensive oversight apply to intelligence in part because of certain statutory and procedural restrictions. These limitations conflict with the general and impressive oversight mandate and authorities included in the Legislative Reorganization Act of 1946 (P. L. 79-601; 60 Stat. 812) and of 1970 (P. L. 91-510; 84 Stat. 1140). This section reviews those authorities in contrast to the protections granted to intelligence agencies, especially the Central Intelligence Agency. The limitations include the concept of executive privilege, certain statutory discretion for agency protection of intelligence sources and methods, and restrictions on the accounting and auditing of intelligence expenditures. Congressional oversight ingredients include the mandate and jurisdiction of committees; staffing, funding and supportive services; subpoena/contempt powers; immunity granting authority; and disclosure/classification of materials rulings.

Mandate: The "continuous watchfulness" mandate provided by the 1946 Legislative Reorganization Act was supplemented by a requirement in the 1970 counterpart that "each standing committee... shall review and study, on a continuing basis, the application, administration, and execution of those laws, or parts of laws, the subject matter of which is within the jurisdiction of that committee."

The most generous oversight authority is that granted to the Joint Committee on Atomic Energy (JCAE), which oversees the Energy and Development Administration, 13/ among the intelligence agencies. Sec. 2252 (a), Title 42 of the United States Code provides that...

13/ For interpretations of this oversight power, see Joseph Harris, op. cit. and Harold Green and Alan Rosenthal, Government of the Atom: The Integration of Powers (New York: Atherton, 1963).

> (a) The Joint Committee shall make continuing studies of the activities of the Atomic Energy Commission and of problems relating to the development, use, and control of atomic energy. During the first ninety days of each session of the Congress, the Joint Committee may conduct hearings in either open or executive session for the purpose of receiving information concerning the development, growth, and state of the atomic energy industry. The Commission shall keep the Joint Committee fully and currently informed with respect to all of the Commission's activities. The Department of Defense shall keep the Joint Committee fully and currently informed with respect to all matters within the Department of Defense relating to the development, utilization, or application of atomic energy. Any Government agency shall furnish any information requested by the Joint Committee with respect to the activities or responsibilities of that agency in the field of atomic energy.

Another example of the oversight mandate is that affiliated with special investigative efforts, such as the Senate Select Committee on Presidential Campaign Activities. The broad responsibility of the select committee was contained in S. Res. 60, accepted on Feb. 7, 1973:

> To establish a select committee of the Senate to conduct an investigation and study of the extent, if any, to which illegal, improper, or unethical activities were engaged in by any persons, acting individually or in combination with others, in the presidential election of 1972, or any campaign, canvass, or other activity related to it.

This charge was refined in later sections to encompass specific inquiry areas but permitted enough flexibility for a preliminary inquiry into the role and activities of certain intelligence agencies, especially the CIA, FBI, and IRS.

The authority of the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities is modeled along lines similar to that of the Select Committee on Presidential Campaign Activities in terms of general responsibility and detailed inquiry areas. The Senate select committee on intelligence is empowered "to conduct an investigation and

study of governmental operations with respect to intelligence activities and of the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency of the Federal Government or by persons, acting individually or in combination with others, with respect to any intelligence activity carried out by or on behalf of the Federal Government." (S. Res. 21) The House counterpart was granted an even broader statement of purpose-- "to conduct an inquiry into the organization, operations, and oversight of the intelligence community of the United States Government." (H. Res. 138) Both House and Senate select committees possess more detailed provisions, defining specific areas of inquiry. As with most select committees, those on intelligence possess only investigative/oversight authority, not legislative nor authorizing authority.

Jurisdiction: The jurisdiction of committees with respect to intelligence agencies and activities varies considerably. Certain standing committees, especially Appropriations and Armed Services, possess extensive oversight jurisdiction in terms of the number of agencies and the extent of activities covered. Others are restricted to one agency and/or to certain activities. The select committees on intelligence are the first nonappropriations committees to be granted comprehensive jurisdiction with respect to intelligence in the post World War II era.

Staff, Funds, and Support Services: Sufficient professional staff and adequate funding are critical to oversight and investigations because of the extensive and often routine duties and responsibilities associated with the functions. Sec. 202(a) and (c) of the 1970 Legislative Reorganization

Act authorize each standing committee to employ a regular staff of six professional and six clerical assistants. (Sec. 202(b) exempts the Committee on Appropriations from this restriction.) However, additional permanent staff may be provided by public law or chamber resolution.

Besides authorizations for additional permanent staff, several procedures provide for supplemental committee staff -- use of extra-Congressional personal, contracting for private consulting services, and the employment of investigative personnel. Contracting for private consulting/research services is authorized by the 1970 Legislative Reorganization Act and the Congressional Budget and Impoundment Act of 1974 (P. L. 93-344; 88 Stat. 297).

Extra-Congressional staff are of two types -- Federal executive personnel and personnel of the agencies affiliated with the Congress (i.e., General Accounting Office (GAO), Congressional Research Service (CRS), Congressional Budget Office (CBO) and Office of Technology Assessment (OTA). Committees may "borrow" staff from executive agencies. One of the most prominent examples had been the use of FBI agents as investigators for the House Committee on Appropriations during the 1950's. 14/

Certain congressional instrumentalities -- GAO, CBO, CRS -- provide direct staff support to committees. Sec. 235 of the 1970 Legislative Organization Act provides for the assignment of GAO personnel on a full-time, continuing basis not to exceed one year with the stipulation that the

14/ Cited in Congressional Quarterly Weekly Report, July 23, 1971, p. 1565. Also see Richard Fenno, The Power of the Purse: Appropriations Politics in Congress (Boston: Little, Brown and Co., 1966), pp. 152-155.

appropriate committee will reimburse GAO for the salary of each employee assigned to the committee. Sec. 321(e) of the same statute authorizes that CRS employees be made "available for special work with the committees and Members..." for certain duties, some of which relate to oversight. The wording of the section allows for a flexible relationship between CRS and committees in terms of assignments and reimbursement. CBO, the most recently created congressional service agency, is required to assist committees in its organic statute, the 1974 Budget and Impoundment Control Act (P.L. 93-344; 88 Stat. 297). 15/ Sec. 202(d) of the statute provides that CBO may assign personnel at the request of a committee to assist with certain information pertaining to budget authority and tax expenditures as well as revenues, receipts, estimated future revenues, and changing revenue conditions.

The congressional agencies also provide a variety of supportive or supplemental services for the Congress, which relate to the oversight function. The Congressional Budget Office is authorized to provide budget projections and analyses regarding executive agencies and departments. However, current access to necessary statistical data regarding intelligence agency budgets is severely constrained, thus, limiting the effectiveness of CBO in this regard

The Congressional Research Service received an expanded oversight mandate under sec. 321 of the 1970 Legislative Reorganization Act. That capability is available to standing committees and members of Congress

15/ The priority committee assignment for CBO personnel is with the Budget Committees to which "personnel of the Office shall be assigned... (vis-a-vis)...any other committee (to which) personnel of the Office may be assigned..." (emphasis added) Sec. 202(d), P.L. 93-344, the Budget and Impoundment Control Act of 1974.

in the area of intelligence oversight. Background reports, historical and policy analyses, and supplemental staff assistance are some of the activities which CRS provides.

The Office of Technology Assessment, established on October 13, 1972 by the Technology Assessment Act (P. L. 92-484; 86 Stat. 797), might provide oversight support in the area of intelligence. The Office is mandated "to provide early indications of the probable benefits and adverse impacts of applications of technology and to develop other coordinate information which may assist the Congress," a responsibility which might include an appraisal of technological developments regarding intelligence production.

The General Accounting Office is well-known for its oversight function, relating to its auditing and accounting duties. 16/ However, the authority granted to the Comptroller General, the director of the GAO, by the 1921 Budget and Accounting Act, as amended (31 U.S.C. 42 et seq.) is restricted in terms of intelligence agencies for several reasons -- lack of agency cooperation, legal restrictions on GAO authority, and legal security protections for intelligence agencies. Since agency cooperation is a precondition for an effective and comprehensive audit, the absence of cooperation limits GAO efforts. For example, recently GAO has conducted the

16/ For a review of the history and functions of the Office, see Richard Brown, The GAO: Untapped Source of Congressional Power (Knoxville, Tenn.: University of Tennessee Press, 1970); Thomas D. Morgan, "The General Accounting Office: One Hope for Congress to Regain Parity of Power with the President," North Carolina Law Review, vol. 51 (Oct. 1973); Fred Kaiser, "The Comptroller General: History and Independence," a report from the Congressional Research Service for the Senate Committee on Government Operations, Subcommittee on Reports, Accounting, and Management, GAO Legislation. (Hearings, 94th Congress, 1st session, Oct. 2, 1975) (Washington, D.C.: U.S. Govt. Print. Off., 1975), pp. 112-131. Another important source is hearings held by the House Select Committee on Intelligence, U.S. Intelligence Agencies and Activities: Intelligence Costs and Fiscal Procedures (94th Congress, 1st session, 1975) (Washington, D.C.: U.S. Govt. Print. Off., 1975).

first investigation of FBI activities and procedures in the history of the Bureau, an examination delayed in large part because of the opposition of the late FBI Director J. Edgar Hoover. 17/

Restrictions affecting GAO audit of the CIA have also been evident. According to one analysis, GAO had once performed comprehensive audits of the CIA, covering not only the expenditure of funds but also the efficency and economy of utilization of property and personnel. 18/ However, since 1961 GAO has "not conducted any reviews at the CIA nor any reviews which focus specifically on CIA activities," according to a letter from the Acting Comptroller General to Senator William Proxmire in 1974. 19/

Statutory restrictions on GAO investigative, audit, and accounting functions are of two types. GAO audits are confined to public funds, and confidential and covert funding of some intelligence agency activities precludes GAO accounting and auditing. Sec. 321(a) of the 1921 Budget and Accounting Act, as amended (31 U. S. C. 53) provides that...

> The Comptroller General shall investigate, at the seat of government or elsewhere, all matters relating to the receipt, disbursement, and application of public funds... he shall make recommendations looking to greater economy or efficiency in public expenditures. (emphasis added)

17/ Commencing the investigation in Dec. 1974. a GAO spokesman said, "we (GAO) always believed we had the authority to conduct an investigation into FBI activities but the late FBI chief, J. Edgar Hoover, just wouldn't approve of it. And without the cooperation of the agency involved, there's no way we can conduct a proper investigation." Reported by Ronald Koziol, "Intensive Investigation of FBI Underway," Los Angeles Times, Dec. 22, 1974, Part 1, p. 5.

18/ Robin Schwartzman, "Fiscal Oversight of the Central Intelligence Agency: Can Accountability and Confidentiality Coexist?" New York University Journal of International Law and Politics, vol. 7, no. 3 (Winter 1974), p. 528.

19/ Ibid., p. 518.

Consequently, nonappropriated funds are subject to only limited audit by the GAO. The following statement prepared by the Office of General Counsel of the General Accounting Office describes this restriction and its ramifications:

> There are many activities carried on by Government Agencies which are subject to limited audit by the General Accounting Office because they are financed with nonappropriated funds. These activities include the operation of exchanges, restaurants, concessions, canteens, welfare activities, vending machine operations, and other revenue-producing activities.
>
> Over the years these activities have grown to the status of big business. In general, they are carried on for the morale, welfare, and recreation of the agency or military establishment. GAO authority to audit these activities is limited to those aspects in which they receive support from appropriated funds, such as the use of Government buildings, the services of military personnel, and the like.
>
> Under existing legislation, these activities are not within the reach of an effective audit by the General Accounting Office. This Office has in the past advocated a modification of its audit jurisdiction and the entire subject of the inadequacy of present-day controls over some of these revenue-producing activities has been brought to the attention of the Congress on a number of occasions.
>
> The Comptroller General's report to the Congress (B-45101) dated August 10, 1949, provides a fairly complete disclosure of the situation. 20/

Intelligence agencies may engage in revenue-producing activities and conduct operations which are financed with nonappropriated funds. The operations of Air America by the Central Intelligence Agency might be a possible inclusion which would receive only a limited audit by GAO under current authority. Victor Marchetti and John Marks in The CIA and the Cult of Intelligence devote a chapter to the proprietary organizations operated by the Agency. 21/ These proprietary organizations include various

20/ Office of General Counsel, U.S. General Accounting Office, Legislation Relating to the Functions and Jurisdiction of the General Account-Office (including legislation through the 92d Congress), Jan. 1973.

21/ Victor Marchetti and John D. Marks, The CIA and the Cult of Intelligence (New York: Dell Publishing Co., 1974), pp. 146-165.

air transport companies and other corporations, according to the authors, which generate revenue for the Agency and/or rely upon nonappropriated funding to some extent, thus, effectively excluding them from the GAO audit capacity.

A second type of restriction on GAO authority is included in appropriations statutes for various intelligence agencies. Confidential funds assigned to agencies are accounted for solely on the certificate of the agency head or departmental Secretary (e.g. FBI confidential funds are expended under the authority of the Attorney General and accounted for solely under his certificate). Authority for confidential funding exists for various purposes, some of which are likely to involve intelligence functions. A specific example of this is found regarding Navy intelligence in provisions in the Naval Service Appropriation Act for fiscal year 1917, approved August 29, 1916 (P.L. 64-241; codified in 31 U.S.C. 108):

> Expenditures by the Department of the Navy from the appropriation for obtaining information from abroad and at home shall be accounted for specifically, if, in the judgment of the Secretary of the Navy, they may be made public, and he shall make a certificate of the amount of such expenditures as he may think it advisable not to specify, and every such certificate shall be deemed a sufficient voucher for the sum therein expressed to have been expended.

Furthermore, GAO accounting and audit authority is limited by statutory security protections for some intelligence agencies. Regarding the CIA, the Central Intelligence Agency Act of 1949 (P.L. 81-110), which amended the Agency's establishing authority included in the National Security Act of 1947 (P.L. 80-253, 61 stat. 495), provided that funds made available to the Agency "may be expended without regard to the provisions

of law and regulations relating to the expenditure of Government funds..." Covert financing and the use of confidential funds under this authority have largely precluded independent GAO accounting and comprehensive audits. 22/ Yet there have been occasions of GAO activity in this area. On-site compliance audits were conducted by GAO in 1949 at the request of the Director of Central Intelligence, who has authority to extend GAO activities in this regard. From 1959 until 1961, GAO conducted comprehensive audits of the Agency. Moreover, other sensitive intelligence agencies are not as protected from GAO audit authority. The National Security Agency, a part of the Department of Defense, routinely undergoes GAO audits. (The results of the audits are not published in compliance with Public Law 86-36 (73 Stat. 63, passed on May 29, 1959), which forbids disclosure of any information regarding NSA activities.) According to a GAO statement on the subject of intelligence agency audits, 23/ the General Accounting Office has recently expanded its audit capacity with regard to NSA to include continuous compliance audits of NSA vouchers and accounts. These audits are conducted on NSA premises or at designated records storage sites where the confidentiality of the documents could be maintained. 24/

Another inhibition on GAO investigative authority regarding intelligence relates to security clearance procedures rather than statutory protections. The security clearance for GAO investigative personnel instituted by intelligence agencies is not automatically interchangeable among the agencies.

22/ See Louis Fisher, op. cit., pp. 214-221 for a discussion of CIA spending powers.

23/ The GAO statement was included in a letter prepared by the Acting Comptroller General for Senator Proxmire in 1974. Citation supra note 18, p. 528.

24/ Ibid.

Subpoena/Contempt Powers: One of the critical oversight authorities possessed by the Congress is the power to issue the subpoena, the formal authority to require the attendance and testimony of witnesses and the production of documents and materials at the behest of duly authorized committees. That authority is currently provided in sec. 134(a) of the 1946 Legislative Reorganization Act, as amended -- "Each committee... including any subcommittee of any such committee, is authorized to hold hearings...to require by subpoena or otherwise the attendance of such witnesses and the production of such correspondence, books, papers, and documents, to take such testimony...as it deems advisable."

Enforcement of the subpoena power is based upon provisions for contempt of Congress citations found in sections 192 of 194 and Title 2 of the United States Code. The relevant passages follow:

192. Refusal of Witness to Testify or Produce Papers

> Every person who having been summoned as a witness by the authority of either House of Congress to give testimony or to produce papers upon any matter under inquiry before either House, or any joint committee established by a joint or concurrent resolution of the two Houses of Congress, or any committee of either House of Congress, willfully makes default, or who, having appeared, refuses to answer any question pertinent to the question under inquiry, shall be deemed guilty of a misdemeanor, punishable by a fine of not more than $1,000 nor less than $100 and imprisonment in a common jail for not less than one month nor than twelve months. (R.S. § 102; June 22, 1938, ch. 594, 52 Stat. 942.)

194. Certification of Failure To Testify; Grand Jury Action

> Whenever a witness summoned as mentioned in section 192 of this title fails to appear to testify or fails to produce any books, papers, records, or documents, as required, or whenever any witnesses so summoned refuses to answer any question pertinent

> to the subject under inquiry before either House, or any joint committee established by a joint or concurrent resolution of the two Houses of Congress, or any committee or subcommittee of either House of Congress, and the fact of such failure or failures is reported to either House while Congress is in session, or when Congress is not in session, a statement of fact constituting such failure is reported to and filed with the President of the Senate or the Speaker of the House, it shall be the duty of the said President of the Senate or Speaker of the House, as the case may be, to certify, and he shall so certify, the statement of facts aforesaid under the seal of the Senate or House, as the case may be, to the appropriate United States attorney, whose duty it shall be to bring the matter before the grand jury for its action. (R.S. §104; July 13, 1936, ch. 884, 49 Stat. 2041; June 22, 1938, ch. 594, 52 Stat. 942.)

Sec. 192 of Title 2, noted above, provides the statutory contempt procedure. This provision does not preempt, however, Congress' nonstatutory common law contempt power, known as the inherent contempt power. This inherent power was first used in 1795 and given judicial recognition in 1821. In Anderson v. Dunn, 19 U.S. (6 Wheat.) 204 (1821), the Supreme Court upheld the right of either House to attach and punish a person other than a Member of Congress for contempt of its authority, without using the judicial process. The inherent power of Congress to punish for contempt was last exercised in 1934 and the authority of the Senate to try the charge of contempt before its bar was upheld by the Supreme Court in Jurney v. MacCracken, 294 U.S. 125 (1935).

A third type of contempt power potentially available to congressional committees is the civil contempt citation. Civil contempt authority provides a procedure whereby a committee may prosecute for contempt directly in the Federal courts rather than through the parent chamber, as is required for criminal contempt citations. Civil contempt, however, is not presently authorized.

25/ For elaboration see Samuel Dash, Chief Counsel, David Dorsen, and Ronald D. Rotunda, "The Congressional Contempt Power," (memorandum) in Senate Select Committee on Presidential Campaign Activities, Appendix to the Hearings: Legal Documents Relating to the Select Com-

Two obvious points of contention regarding the subpoena/contempt power of the Congress and intelligence oversight are the doctrine of executive privilege and prohibitions against lower echelon intelligence officials testifying before congressional committees. The latter conflict was noted in the previous section and relates to procedural and, in some cases, statutory restrictions. The authority granted to the Director of Central Intelligence to protect "intelligence sources and methods from unauthorized disclosure" (in the National Security Act of 1947) is a case in point.

Executive privilege refers to the order of the President preventing disclosure of material or information, the release of which he may judge to be detrimental to the national security. Various types of executive privilege have been noted by the Supreme Court in determining the constitutionality of the President's claim in response to legitimate congressional needs for information and documentation. Since judicial intervention into this area is most recent, beginning in the Watergate era, it is unclear how far executive privilege and competing congressional claims utilizing the subpoena power extend. In United States v. Nixon, 418 U.S. 683 the Supreme Court intimated that military, diplomatic, or sensitive national security material might not be subject to congressional demands and might be protected by the claim of executive privilege. 26/ Such a decision might

mittee Hearings, Part I, 93d Congress, 2d session (Washington, D.C.: U.S. Govt. Print. Off., 1974), pp. 75-102; Ronald Goldfarb, The Contempt Power (Garden City, New York: Anchor Books, 1971); and Carl Beck, Contempt of Congress (New Orleans: Phauser, 1959).

26/ United States v. Nixon, 418 U.S. 683 (1974), while rejecting an unqualified presidential privilege of immunity from judicial process in a criminal proceeding, sustains the existence of the Executive privilege "to the extent [it] relates to the effective discharge of a President's powers..." 418 U.S. at 711.

"In this case the President challenges a subpoena served on him as a third party requiring the production of materials for use in a criminal prosecution; he does so on the claim that he has a privilege against disclosure of confidential communications. He does not place his claim of privilege on the ground they are military or diplomatic secrets. As to those areas of Art. II duties the courts have traditionally shown the utmost deference to Presidential responsibilities. In C & S Air Lines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948), dealing with Presidential authority involving foreign policy considerations, the Court said:

'The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs has available intelligence services whose reports are not and ought not to be published to the world. It would be intolerable that courts, without the relevant information should review and perhaps nullify actions of the Executive taken on information properly held secret.'

"In United States v. Reynolds, 345 U.S. 1 (1953), dealing with a claimant's demand for evidence in a damage case against the Government the Court said:

'It may be possible to satisfy the courts from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged. When this is the case, the case, the occasion for the privilege is appropriate, and the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone in chambers.' Id., at 10.

"No case of the Court, however, has extended this high degree of deference to a President's generalized interest in confidentiality. Nowhere in the Constitution, as we have noted earlier, is there any explicit reference to a privilege of confidentiality, yet to the extent this interest relates to the effective discharge of a President's powers, it is constitutionally based." Id., at 710-711.

For a review of the complexities and constitutionality of executive privilege, see Raoul Berger, Executive Privilege: A Constitutional Myth (Cambridge, Mass.: Harvard University Press, 1974); Adam Carlyle Breckenridge, The Executive Privilege: Presidential Control over Information (Lincoln, Nebraska: University of Nebraska Press, 1974); and Mary Louise Ramsey, "Executive Privilege: Withholding Information from the Congress--Selected Issues and Judicial Decisions," Congressional Research Service Multilith 75-127A (April 3, 1975). Recent court decisions are Senate Select Committee on Presidential Campaign Activities v. Nixon, (C.A.D.C.) 498 F. 2d 725 (1974), in addition to United States v. Nixon, 418 U.S. 683 (1974).

well depend on the determination of how compelling are the congressional needs for such information. Judicial resolution of the conflict between congressional subpoena and executive privilege powers are likely to remain on a case by case basis. Suffice it to say, that intelligence documents, materials, and information are some of the most likely candidates for the imposition of executive privilege because of the intimate relationship of intelligence with national security.

Political rather than judicial resolution of the competing claims has been the norm and has been manifested recently. Certain information regarding intelligence activities, operations, financing, and expenditures was received by the Select committees on intelligence based upon informal agreements with the President rather than through court proceedings, although the House Select Committee voted to bring contempt citations against Secretary of State Kissinger for refusing to produce documents concerning covert CIA operations and alleged Soviet Union violations of arms-control agreements. The contempt citations were later dismissed by the Committee when it had obtained "substantial compliance" with its request. 27/

Another conflict with Congress' subpoena/comtempt power is implicit in the establishing legislation for the Central Intelligence Agency. The National Security Act of 1947 (P.L. 80-253; 61 Stat. 495) provides the

27/ Committee action reported by Murrey Marder, "Contempt Citations Eased," Washington Post, Dec. 12, 1975, p. A1. House Select Committee on Intelligence, "Proceedings Against Henry A. Kissinger," 94th Congress, 1st session. Dec. 10, 1975, House Rept. no. 94-693.

following authority for the Director of Central Intelligence:

> Sec. 102(d)(3)...And provided further, That the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure.

This provision not only requires central clearance for statements made by Agency officials but may preclude their testimony before congressional committees. Presently, the Director of Central Intelligence testifies befor congressional committees but the Comptroller and Inspector General of the Agency, important officials regarding the internal operations of the Agency for comprehensive oversight, are not customary witnesses. Moreover, this section of the National Security Act of 1947 delegates a great deal of discretion to the Director in determining access to Agency documents and materials for some congressional investigators.

Immunity for Witnesses: Besides restrictions imposed by executive privilege and/or intelligence agency clearance, testimony from agency officials may be limited by the possibility of incrimination of a witness. The 5th Amendment of the Constitution may be exercised by a witness to prevent self-incrimination. Recognizing this protection, Congress possesses the authority to grant immunity to a witness, a power which may be asserted independently by the committees of Congress. Sec. 6002 of Title 18, United States Code, codifies the statutory basis for granting immunity.

> §6002. Immunity generally.
>
> Whenever a witness refuses, on the basis of his privilege against self-incrimination, to testify or provide other information in a proceeding before or ancillary to --
> (1) a court or grand jury of the United States
> (2) an agency of the United States, or
> (3) either House of Congress, a joint committee of the two Houses, or a committee or a subcommittee of either House,
> and the person presiding over the proceeding communicates to the witness an order issued under this part, the witness may not refuse to

comply with the order on the basis of his privilege against self-incrimination; but no testimony or other information compelled under the order (or any information directly or indirectly derived from such testimony or other information) may be used against the witness in any criminal case, except a prosecution for perjury, giving a false statement, or otherwise failing to comply with the order. (Added Pub. L. 91-452, title II, §201(a), Oct. 15, 1970, 84 Stat. 927.)

Such authority may be critical in investigations of alleged criminal misconduct or abuse of authority on the part of agencies and/or in securing testimony of present CIA officers who may violate the "unauthorized disclosure" provision in the National Security Act of 1947.

Disclosure of Materials: Congressional disclosure of classified materials, documents, and information has been one of the controversial segments of the intelligence investigations conducted by the select committees on intelligence. Release of the final investigative report of the House Committee on Intelligence, which included classified material and which was objected to by the executive branch, has been prevented by a House vote of 246-124.28/ This action highlights the inherent controversy surrounding congressional disclosure of material which has been deemed confidential or secret by the executive.

The controversy, however, is not recent but is part of a long-term concern. With the establishment of the select committees on intelligence

28/ The House vote came Jan. 29 on an amendment to a resolution, H. Res. 982, from the House Rules Committee, authorizing the select committee to file its final report by Jan. 30, 1976 but precluding its release until it "has been certified by the President as not containing information which would adversely affect the intelligence activities of the CIA" or other agencies. On Jan. 28, the Rules Committee accepted the amendment proposed by Rep. John Young. Previously, on Jan. 23, the select committee had voted to release the report, which was then submitted to the Rules Committee. Congressional Record. vol. 122, Jan. 29, 1976, pp. H505-H514.

came provisions for preventing unauthorized disclosures. S. Res. 21, which created the Senate select committee, authorized the following disclosure and security clearance provisions to safeguard material under its domain:

> Sec. 7. The select committee shall institute and carry out such rules and procedures as it may deem necessary to prevent (1) the disclosure, outside the select committee, of any information relating to the activities of the Central Intelligence Agency or any other department or agency of the Federal Government engaged in intelligence activities, obtained by the select committee during the course of its study and investigation, not authorized by the select committee to be disclosed; and (2) the disclosure, outside the select committee, of any information which would adversely affect the intelligence activities of the Central Intelligence Agency in foreign countries or the intelligence activities in foreign countries of any other department or agency of the Federal Government.
>
> Sec. 9. No employee of the select committee or any person engaged by contract or otherwise to perform services for the select committee shall be given access to any classified information by the select committee unless such employee or person has received an appropriate security clearance as determined by the select committee. The type of security clearance to be required in the case of any such employee or person shall, within the determination of the select committee, be commensurate with the sensitivity of the classified information to which such employee or person will be given access by the select committee.

The House select committee followed with identical provisions in H. Res. 138, relating to the safeguarding of material and including the caveat "to prevent disclosure...of any information...not authorized by the committee to be disclosed..."

Another committee which is intimately involved with classified and sensitive material and oversees certain intelligence activities and agencies is the Joint Committee on Atomic Energy. Relevant authorities were included in the 1954 amendments to the Atomic Energy Act (P. L. 83-703; 68 Stat. 957). Sec. 206 provides that "the Joint Committee may classify information originating within the committee in accordance with standards used generally

by the executive branch for classifying Restricted Data or defense information." Sec. 207 of the same legislation continues by requiring that "all Committee records, data, charts, and files...shall be kept...under security safeguards as the Joint Committee shall determine in the interest of the common defense and security."

The congressional concern for protection of confidential materials has a long heritage and can be found in Jefferson's Manual. Senate Rule XXXVI provides for executive sessions and procedures for releasing confidential information. The relevant sections of Senate Rule XXXVI follow:

[36.3] 3. All confidential communications made by the President of the United States to the Senate shall be by the Senators and the officers of the Senate kept secret; and all treaties which may be laid before the Senate, and all remarks, votes, and proceedings thereon shall also be kept secret, until the Senate shall, by their resolution, take off the injunction of secrecy, or unless the same shall be considered in open Executive session. [Jefferson's Manual, Sec. LII.]

On Mar. 21, 1885, the Senate agreed to the following:

Ordered, That the injunction of secrecy be removed from the following report from the Committee on Rules, viz:

The Committee on Rules, to which was referred a question of order raised by the Senator from Maine (Mr. Fyre) as to the operation of clause 3, Rule XXXVI, reported that it extends the injunction of secrecy to each step in the consideration of treaties, including the fact of ratification; that the secrecy as to the fact or ratification of a treaty may be of the utmost importance, and ought not to be removed except by order of the Senate, or until it has been made public by proclamation by the President. (S. Ex. Jour. 20, 49 special, Mar. 21, 1885.)

On Feb. 8, 1900, the Senate agreed to the following:

Ordered, Whenever the injunction of secrecy shall be removed from any part of the proceedings of the Senate in Executive session, or secret legislative session, the order of the Senate removing the same shall be entered by the Secretary in the Legislative Journal as well as in the Executive Journal, and shall be published in the Record. (S. Jour. 131, 56-1, Feb. 8, 1900.)

[36.4] 4. Any Senator or officer of the Senate who shall disclose the secret or confidential business or proceedings of the Senate shall be liable, if a Senator, to suffer expulsion from the body; and if an officer, to dismissal from the service of the Senate, and to punishment for contempt.

[36.5] 5. Whenever, by the request of the Senate or any committee thereof, any documents or papers shall be communicated to the Senate by the President or the head of any department relating to any matter pending in the Senate, the proceedings in regard to which are secret or confidential under the rules, said documents and papers shall be considered as confidential, and shall not be disclosed without leave of the Senate.

Senate Rule 36.3 develops Senate chamber procedures with respect to disclosure of confidential or classified material in its possession. A Senate resolution, S. Res 280, adopted in 1972 provided reinforcement that such disclosures were internal matters of the Senate and that judicial interference should be precluded. S. Res. 280 was in response to a Supreme Court case involving Senator Mike Gravel and his release of then-classified segments of the "Pentagon Papers." The Senate, which voted to pay for Senator Gravel's expenses resulting from the case, resolved that...

> This case necessarily involves the right of the Senate to govern its own internal affairs and to determine the relevancy and propriety of legislative activity and the scope of a senator's duties under the rules of the Senate and the Constitution...A decision in this case may impair the constitutional separation of powers between legislative branch and executive and judicial branches of government.

The Supreme Court in the ensuing decision, Gravel v. United States, 408 U.S. 606 (1972), did rule that Senator Gravel must testify before a Federal grand jury regarding disposition of the "Pentagon Papers" to Beacon Press, private publishers of the papers, but not about the subcommittee meeting at which the material was released. The Court decision granting immunity to congressmen in the performance of their legislative duty was based on the Speech and Debate Clause of the Constitution, Art. I, sec. 6, cl. 1, and on the Court's interpretation that the subcommittee meeting fell within a "legitimate legislative sphere." This interpretation of what is included within the legislative sphere was most significantly expanded in Eastland v. United States Servicemen's Fund, Civil Action No. 73-1923 (U.S. Supreme

Court, May 27, 1975), which concluded that the power to investigate and to do so through compulsory processes (i.e. issuance of subpoena in this case) falls within the definition of "legitimate legislative sphere."

The House of Representatives' internal procedures regarding the release of confidential or classified material received in executive session differ somewhat from the Senate's. Most importantly, House Rule 29 establishes relevant procedures but contains no provision insuring the continued confidentiality of that material:

RULE XXIX

SECRET SESSION.

Whenever confidential communications are received fromthe President of the United States, or whenever the Speaker of any Member shall inform the House that he has communications which he believes ought to be kept secret for the present, the House shall be cleared of all persons except the Members and officers thereof, and so continue during the reading of such communications, the debates and proceedings thereon, unless otherwise ordered by the House.

This rule, in a somewhat different form, was adopted in 1792, although secret sessions had been held by the House before that date. They continued to be held at times with considerable frequency until 1830. In 1880, at the time of the general revision of the rules, the House concluded to retain the rule, although it had been long in disuse (V, 7247; VI, 434).

The two Houses have legislated in secret session, transmitting their messages also in secrecy (V, 7250); but the House has declined to be bound to secrecy by act of the Senate (V, 7249). Motions to remove the injunction of secrecy should be made with closed doors (V, 7254). In 1843 a confidential message fromthe President was referred without reading; but no motion was made for a secret session (V, 7255).

By way of summary, the Congress possesses impressive oversight authorities, including statutory mandates to maintain "continuous watchfulness;" internal control over funding, staff, and supportive services, which have been accorded expanded oversight authority and capabilities; and essential powers to gain access to documents and material as well as testimony of witnesses. These powers with regard to intelligence are buttressed

by Constitutional protections of Congress' investigative authority and the handling of confidential or classified material, the latter of which is largely an internal congressional matter. (Because of the absence of statutory authority, Executive Order 11652, issued by President Nixon on March 10, 1972, governs the classification and declassification of national security information. This Presidential power has congressional and judicial sanction. According to the concurring opinion of Mr. Justice Marshall, in New York Times Co. v. United States, 403 U.S. 713, 741 (1971): "...there is no problem concerning the President's power to classify information as 'secret' or 'top secret.' Congress has specifically recognized Presidential authority... to classify documents and information. See, e.g., 18 U.S.C. § 798, 50 U.S.C. § 783.")

On the other hand, there are prohibitions against comprehensive congressional oversight, unique to the intelligence community. These restrictions include the likely incurrence of executive privilege and invocations of statutory protections of certain intelligence sources and methods; intelligence agency security clearance procedures applied to congressional investigators; investigative limitations inherent in GAO's mandate in the 1921 Budget and Accounting Act coupled with agency use of covert and confidential funding, which is exempted from normal audit and accounting procedures; and specific CIA exemptions regarding Agency expenditures.

III. Reorganization Proposals relating to Intelligence Oversight

Proposals to reorganize the congressional oversight structure regarding intelligence have existed for more than two decades and have resulted in congressional votes on several occasions. Although most proposals concentrated on the congressional relationship with the CIA, an increasing number, including most of the current ones, incorporate other intelligence

agencies. The recommendations have come from a variety of sources, including governmental commissions, congressional committees, and individual legislators.

Governmental Commission Recommendations

The first governmental commission to consider congressional oversight of intelligence, specifically with regard to the CIA, was the Commission on the Organization of the Executive Branch of the Government, operating from 1953 to 1955 (the 2d Hoover Commission). The actual investigation into intelligence activities of the Government was conducted by a task force chaired by General Mark W. Clark. 29/ The Clark Task Force recommended a "watchdog" commission, composed of private citizens and representatives of both Houses of Congress and of the President. The specific language of the report, which includes the justification for the recommendation, follows:

> The task force further is concerned over the absence of satisfactory machinery for surveillance of the stewardship of the CIA. It is making recommendations which it believes will provide the proper type of "watchdog" commission as a means of reestablishing that relationship between the CIA and the Congress so essential to and characteristic of our democratic form of government, but which was abrogated by the enactment of Public Law 110 and other statutes relating to the agency. It would include representatives of both Houses of Congress and of the Chief Executive. Its duties would embrace a review of the operations and effectiveness, not only of the CIA, but also of other intelligence agencies.

29/ A summary of the Clark Task Force efforts and recommendations are included in a report of the Committee on Rules and Administration of the Senate, Joint Committee on Central Intelligence (report to accompany S. Con. Res. 2), 84th Congress, 2d session, Feb. 23, 1956 (Senate Report no. 1570), pp. 8-12. The Clark Task Force report was in two parts, one of which was, and remains, classified. The unclassified part of the Clark Task Force is available in the report by the Commission on the Organization of the Executive Branch of the Government (the 2d Hoover Commission, 1953-55), "The Report on Intelligence Activities in the Federal Government," Report to the Congress (Washington, D.C.: U.S. Govt. Print. Off., 1955), Part II, pp. 3-76.

The task force report adds:

> The task force fully realizes that the Central Intelligence Agency, as a major fountain of intelligence for the Nation, must of necessity operate in an atmosphere of secrecy and with an unusual amount of freedom and independence. Obviously, it cannot achieve its full purpose if subjected to open scrutiny and the extensive checks and balances which apply to the average governmental agency.
>
> Because of its peculiar position, the CIA has been freed by the Congress from outside surveillance of its operations and its fiscal accounts. There is always a danger that such freedom from restraints could inspire laxity and abuses which might prove costly to the American people.
>
> Although the task force has discovered no indication of abuse of powers by the CIA or other Intelligence agecies, it nevertheless is firmly convinced, as a matter of future insurance, that some reliable, systematic review of all the agencies and their operations should be provided by congressional action as a checkrein to assure both the Congress and the people that this hub of the Intelligence effort is functioning in an efficient, effective, and reasonabley economical manner. [Emphasis supplied.]
>
> Within the Armed Services Committee, there is a liaison channel between the Congress and CIA which serves a worthy purpose, but which cannot include private citizens in its membership and has not attempted to encompass the wide scope of service and continuity which this task force considers essential for "watchdog" purposes.
>
> The task force recognizes that secrecy is necessary for proper operation of our foreign intelligence activities but is concerned over the possibility of the growth of license and abuses of power where disclosure of costs, organization, personnel, and functions are precluded by law.
>
> On the other hand, sporadic investigations in this field might inadvertently result in unauthorized disclosure of classified information to the detriment of the intelligence effort. Periodic audits or studies by some qualified, impartial agency would remove both of these dangers and would also allay any suspicious and distrust which have developed in the public mind by the complete secrecy of these operations. Such a procedure also might serve to shield our intelligence program from unjustifiable attacks upon the agencies conerned, and enhance public confidence and support of this vital work.
>
> The Central Intelligence Agency Act of 1949 legalized the administrative procedures for the Agency. It was passed by the Congress on the unanimous recommendation of the Armed Services Committee. 30/

The Hoover Commission did not accept the Clark Task Force recommendation regarding a "watchdog" commission on the grounds that a permanent and mixed commission would present difficulties in this sensitive area.

30/ Ibid., p. 11.

Instead, the Hoover Commission recommended in its report transmitted to the Congress on June 29, 1955 two separate entities -- A Presidentially appointed commission and a joint congressional committee:

> (a) That the President appoint a committee of experienced private citizens, who shall have the responsibility to examine and report to him periodically on the work of Government foreign intelligence activities. This committee should also give such information to the public as the President may direct. The Commission should function on a part-time and per diem basis.
> (b) That the Congress consider creating a joint congressional committee on foreign intelligence, similar to the Joint Committee on Atomic Energy. In such case, the two committees, one Presidential and the other, congressional, could collaborate on matters of special importance to the national security. 31/

Two recent governmental commissions have commented on congressional oversight of intelligence and the majority reports of both have recommended the creation of a new congressional committee -- again a joint committee. The President's Commission on CIA Activities Within the United States, chaired by Vice President Nelson Rockefeller (hereafter referred to as the Rockefeller Commission), was created by Executive Order No. 11828 of January 4, 1975, issued by President Ford. After reviewing current oversight efforts of the Congress, the Rockefeller Commission final report, submitted on June 6, 1975, 32/ concluded that...

> Neither the members of the oversight committees nor other members of Congress have generally received detailed information on CIA operations...While it appears that the subcommittees or at least their leaders and the leaders of Congress have been informed of major CIA activities, the amount of information provided does not always correspond with that available to Congress in other sensitive areas.

31/ Ibid., p. 12. The first part of the recommendation, relating to a Presidential advisory commission, led to he creation of the President's Foreign Intelligence Advisory Board, created on Feb. 6, 1956 by Executive Order 10656, issued by President Eisenhower.

32/ President's Commission on CIA activities Within the United States, Report (Washington, D. C.: U. S. Govt. Print. Off., 1975), released June 6, 1975.

> In sum, congressional oversight of the CIA has been curtailed by the secrecy shrouding its activities and budget. At least until quite recently, Congress has not sought substantial amounts of information of a sensitive nature. Correspondingly, the CIA has not generally volunteered additional information. 33/

The Rockefeller Commission, thereupon, recommended that...

> The President should recommend to Congress the establishment of a Joint Committee on Intelligence to assume the oversight role currently played by the Armed Services Committees. 34/

When President Ford proposed reorganization of the CIA and changes in statutory and procedural controls surrounding the Agency on Feb. 18, 1976 (H. Doc. No. 94-374), he adopted the Rockefeller Commission recommendation as follows:

> Congress should seek to centralize the responsibility for oversight of the foreign intelligence community. The more committees and subcommittees dealing with highly sensitive secrets, the greater the risks of disclosure. I recommend that Congress establish a Joint Foreign Intelligence Oversight Committee. Consolidating Congressional oversight in one committee will facilitate the efforts of the Administration to keep the Congress fully informed of foreign intelligence activities.
>
> Any foreign intelligence information transmitted by the Executive Branch to the Oversight Committee, under an injunction of secrecy, should not be unilaterally disclosed without my agreement. Respect for the integrity of the Constitution requires adherence to the principle that no individual member, nor committee, nor single House of Congress can overrule an act of the Executive...(H. Doc. No. 94-374)

The second recent commission to comment upon congressional-intelligence relations was the Commission on the Organization of the Government for the Conduct of Foreign Policy, established by Public Law 92-352

33/ Ibid., p. 76-77.

34/ Ibid., p. 81. A caveat to this recommendation was added by Commission member Erwin Griswold in a footnote on page 81. It recognized that the Commission jurisdiction extended to only domestic CIA activities but "the problems which have arisen in the domestic field cannot be fully understood and evaluated unless they are viewed against the role which the CIA has undertaken to play outside the United States."

(Title VI of the Foreign Relations Authorization Act of 1972) on July 13, 1972 and chaired by Robert D. Murphy (hereafter referred to as the Murphy Commission). The release of the report of the Murphy Commission coincided with that of the Rockefeller Commission in June, 1975. 35/

The Murphy Commission recommended the creation of a Joint Committee on National Security to provide congressional oversight of intelligence, among other duties. The broad responsibilities of this committee are detailed in the Commission report:

> In the Commission's view, a Joint Committee on National Security should be established. It should perform for the Congress the kinds of policy review and coordination now performed in the executive branch by the National Security Council, and provide a central point of linkage to the President and to the officials at the Council. In addition it should take responsibility for Congressional oversight of the Intelligence Community.
>
> The Commission recommends that the Joint Committee be vested with the following specific jurisdictions and authorities:
>
> - Receipt, analysis and referral (along with any recommendations it may consider appropriate) of reports from the President under the War Powers Act.
>
> - Receipt and review of analytic products of the intelligence community.
>
> - Oversight (in conjunction with the executive branch) of the system of information classification discussed above.
>
> - Establishment and maintenance of facilities and procedures for storage and handling of classified information and materials supplied to the Congress.
>
> - Establishment of a code of conduct to govern the handling by Committee members of classified or sensitive information.

35/ Commission on the Organization of the Government for the Conduct of Foreign Policy, Report (Washington, D. C.: U. S. Govt. Print. Off., 1975), released June 27, 1975.

The successful experience of the Joint Committee on Atomic Energy illustrates the usefulness of legislative authority in helping assure a Committee's effectiveness. The Commission does not recommend that the proposed Joint Committee be vested with broad authority to report proposed legislation to the House and Senate. In general, any legislative recommendations of the Joint Committee should be reported to relevant standing committees for their considerations. The Commission finds, however, two narrow and specific areas in which the Joint Committee might usefully have authority to report legislation to the floor of each House as the Joint Committee on Atomic Energy is empowered to do.

We propose that the Joint Committee:

- Consider the creation of a statutory system of information classification, and (if intelligence oversight is assigned to it).

- Be granted authority for annual authorization of funds for the intelligence community. 36/

The Murphy Commission report insisted "that most systematic arrangements for Congressional oversight of the intelligence community are needed on a permanent basis... and that such oversight should be conducted by a Joint Committee of the Congress..." 37/ A Joint Committee on National Security, as envisioned by the Murphy Commission, would be the most appropriate vehicle, according to the report.

> In the event that this Committee is not established, however, the Commission recommends that a Joint Committee on Intelligence be established to assume the task of Congressional oversight of the intelligence community. 38/

36/ Ibid., pp. 208-209.

37/ Ibid., p. 209.

38/ Ibid., p. 210. President Ford's proposal for CIA reorganization and congressional oversight incorporated this recommendation: "In this context, a Congressional requirement to keep the (Joint Foreign Intelligence) Oversight Committee 'fully' informed is more desirable and workable as a practical matter than formal requirements for notification of specific activities to a large number of committees. Specifically, Section 662 of the Foreign Assistance Act, which has resulted in over six committee briefings, should be modified as recommended by the Commission on the Organization of the Government for the conduct of Foreign Policy, and reporting should be limited to the new Oversight Committee." (H. Doc. No. 94-374; Feb. 18, 1976)

Senator Mike Mansfield, a member of the Murphy Commission disagreed with the basic recommendation of a Joint Committee on National Security. Senator Mansfield commented that the arguments advanced by the Commission "do not justify the creation of some amorphous Joint Committee on National Security"39/ and that the suggestions regarding intelligence oversight were too modest:

> Returning to the subject of intelligence, I would strongly emphasize the fact that both the executive and legislative branches have been inexcusably lax in supervising intelligence activities. But I am also disappointed with the Commission's findings in this regard. After giving a brief outline of the "intelligence community" the report goes on to make some modest suggestions which represent little if any advance over the conclusions of the Rockefeller Commission, which had a substantially more restricted mandate. Everything is accepted as given and some delicate tinkering with the machinery apparently is considered a sufficient response to the profound issues which have emerged in this connection...
>
> To accomplish the necessary restructuring of the so-called intelligence community I would look primarily to the Senate Select Committee on Intelligence. Thereafter, I would hope to see the creation of a Joint or Senate Committee on Intelligence, which was first proposed twenty-one years ago. Such a Committee should have the most extensive oversight powers possible, it should include members of more recent vintage in its ranks. There might very well be, moreover a limited term of office (on the order of four to six years) for members serving on such a Committee. 40/

Congressional Recommendations, Historical Review

Congressional proposals to restructure oversight of intelligence have existed since 1948 and number more than 200. Most of the bills have recommended a joint committee, although an increasing number have focused on single chamber units.41/ The first proposal to create a Joint Committee on In-

39/ Ibid., p. 231.

40/ Ibid., pp. 231-232.

41/ For a review of the bills and proposals see John Costa, "Legislation Introduced Relative to the Activities of the Intelligence Agencies, 1947-1972" (updated and revised by Gary Lee Evans), Dec. 15, 1972, Congressional Research Service Multilith number 73-22 F and William Raiford, "Legislation Introduced Relative to the Activities of U.S. Intelligence Agencies: 1973-1974," Feb. 5, 1975, Congressional Research Service Multilith number 75-76 F.

telligence, H. Con. Res. 186, was offered in the House of Representatives on April 21, 1948 by Rep. Devitt. It was not until 1953 that another resolution was proposed, S. Con. Res. 42 offered by Senator Mansfield on July 20, 1953. The number of proposals proliferated and reached a peak in both 1956 and again in 1966, climaxing in votes related to creating new congressional oversight structures.

On Jan. 5, 1955 Senator Mansfield along with 32 co-sponsors proposed S. Con. Res. 2, which provided for the establishment of a Joint Committee on Central Intelligence. The structure, composition, duties, and authorities of this committee were defined in the proposal:

> To establish a Joint Committee on Central Intelligence to be composed of six members from the Senate and six members from the House of Representatives. Of the six members to be appointed from the Senate, three shall be members of the Central Intelligence Agency Subcommittee of the Committee on Appropriations of the Senate, and three shall be members of the Central Intelligence Agency Subcommittee of the Committee on Armed Services of the Senate. Of the six members to be appointed from the House of Representatives, three shall be members of the Central Intelligence Agency Subcommittee of the Committee on Appropriations of the House of Representatives, and three shall be members of the Central Intelligence Subcommittee of the Committee on Armed Services of the House of Representatives.
>
> The Joint Committee shall make continuing studies of the activities of the CIA and of problems relating to the gathering of intelligence affecting the national security and of its coordination and utilization by the various departments, agencies, and instrumentalities of the Government. The CIA shall keep the Joint Committee fully and currently informed with respect to its activities. All bills, resolutions, and other matters in the Senate and the House of Representatives relating primarily to the CIA shall be referred to the Joint Committee.

S. Con. Res. 2 was reported by the Senate Committee on Rules and Administration on Feb. 23, 1956, 42/ debated in the chamber over two days, and defeated on a roll call vote of 27 yeas to 59 nays on April 11, 1956. 43/ On that vote, twelve of the original co-sponsors reconsidered their position and voted against the proposal.

A separate Senate oversight committee was proposed in 1966, initially by Senator Eugene McCarthy on Jan. 24, 1966 (S. Res. 210) and later by Senator Fulbright on July 14, 1966 (S. Res. 283). Senate Foreign Relations considered the resolutions in executive session and reported S. Res. 283 after a favorable 14 to 5 vote (Senate Rept. no. 1371). The chamber vote which affected S. Res. 283 was not on the proposal per se but on a point of order raised by Senator Russell (i.e. that under Rule XXV, the resolution consisted of matter predominantly under the jurisdiction of Armed Serrvices and was improperly before the Senate). Senator Russell's point of order was sustained by a vote of 61 yeas to 28 nays on July 14, 1966 and the proposal was referred to Armed Services. 44/ S. Res. 283 follows:

> To create a Committee on Intelligence Operations composed of 9 members -- 3 from Appropriations, 3 from Armed Services, and 3 from Foreign Relations -- to keep currently informed of the activities of the Central intelligence Agency, the Defense Intelligence Agency, the Bureau of Intelligence and Research of the Department of State, and the activities of other agencies relating to foreign intelligence or counterintelligence.

42/ Senate Report no. 1570, cited supra note 29.

43/ Senate debates: Congressional Record, v. 102, April 9, 1956: 5890-91, 5922-39; Congressional Record, v. 102, April 11, 1956: 6047-6063, 6065, 6067-6068. See John Costa, op. cit.

44/ See John Costa, op. cit., p. 28-29 for chronology and vote tabulation. Senate Armed Services failed to report out the proposal.

Current Congressional Recommendations

The commencement of the 94th Congress witnessed the creation of Senate and House select committees on intelligence to investigate allegations of abuse of authority and illegal or unethical conduct on the part of intelligence agencies, principally the CIA.45/ The select committees and their authorities have been commented upon extensively in previous sections. It is sufficient to note here that the select committees marked establishment of the first congressional oversight unit (except for the Appropriations Committees, of course) with comprehensive jurisdiction over intelligence agencies.

With the expiration of the select committees on intelligence scheduled for early 1976, proposals were advanced for new permanent standing committees on intelligence oversight. Elaboration of these proposals and other reform-reorganization recommendations are available in the hearings conducted by Senate Government Operations, in reports of various commissions and committees, and in several law reviews and scholarly treatises.46/

Both select committees were empowered to report out recommendations for the creation of a new oversight unit. The House Select Committee on

45/ Citations supra note 3.

46/ Anon., "The CIA's Secret Funding and the Constitution," Yale Law Journal, vol. 84, no. 3 (Jan. 1975); Committee on Civil Rights of the Association of the Bar of the City of New York, "Military Surveillance of Civilian Political Activities: Report and Recommendations for Congressional Action," The Record of the Association of the Bar of the City of New York, vol. 28 (Oct. 1973); _____, "The Central Intelligence Agency: Oversight and Accountability," (available directly from Association) March 1975; Stanley N. Futterman, "Toward Legislative Control of the C.I.A." New York University Journal of International Law and Politics, vol. 4 (1971); Harry Howe Ransom, The Intelligence Establishment (Cambridge, Mass.: Harvard University Press, 1970), especially Chapter 7; Robin Schwartzman, op. cit.; and Senate Committee on Government Operations, Proposals to Strengthen Congressional Oversight of the Nation's Intelligence Agencies, Hearings, 93d Congress, 2d session, Dec. 9 and 10, 1974 (Washington, D.C.: U.S. Govt. Print. Off., 1975).

Intelligence approved a proposal to create a permanent House committee on intelligence with legislative and oversight authority over government agencies and departments engaged in foreign or domestic intelligence.47/ The Senate counterpart did not formally approve a recommendation but its chairman, Senator Frank Church, and seven other members sponsored S. 2893, a proposal designed to create a Senate Committee on Intelligence Activities with jurisdiction and prior review provisions over the "national intelligence" community (i.e., CIA, NSA, DIA, intelligence compents in the Department of Defense, and the intelligence activities of FBI, among others).48/

Other proposals have been offered during hearings held by Senate Government Operations, which have elicited testimony and further recommendations.49/ Testimony was received from a variety of sources including former Directors of Central Intelligence Richard Helms and William Colby; Secretary of State Kissinger, who advocated a joint oversight panel; Senators

47/ House Select Committee on Intelligence, Recommendations of the Final Report, 94th Congress, 2d session, Feb. 11, 1976 (House Report No. 94-833).

48/ The co-sponsors are Senators Hart (of Michigan), Mondale, Huddleston, Mathias, Schweiker, Morgan, and Hart (of Colorado). S. 2 93 was introduced Jan. 29, 1976. Congressional Record, vol. 122, Jan. 29, 1976, pp. S 756-S 764. The select committee's vice chairman, Senator John Tower, is opposed to any oversight reorganization at this time and "as drafted... because I (Tower) believe serious analysis will reveal it to be both a premature and a simplistic solution to an extremely complicated set of problems." Cited in Congressional Quarterly Weekly, Jan. 24, 1976, p. 198.

49/ Hearings have been held on S. Con. Res. 4, introducted 1/23/75 by Senator Hathaway, creating a Joint Committee on Information and Intelligence; on S. 189, 1/16/75 by Senator Nelson (for himself and Senators Jackson and Muskie), a Joint Committee on the Continuing Study of the Need to Reorganize the Departments and Agencies Engaging in Surveillance; and S. 317, 1/23/75 by Senator Baker, et al., a Joint Committee on Intelligence Oversight but including certain legislative duties as well as oversight. Senators Goldwater, Thurmond, and Tower have advocated no new oversight panel. A report favoring the creation of a Senate Committee on Intelligence has been released by the Senate Committee on Government Operations, "Senate Committee on Intelligence Activities," Report, 94th Congress, 2d session, March 1, 1976 (Senate Report no. 94 -675).

Church, Mansfield, Tower, Thurmond, and Goldwater; and Representatives Aspin, Harrington, and Beard. The various proposals and recommendations encompass both joint and single chamber units, varying membership patterns, and variety of authorities ranging from basic monitoring activities, to prior review of certain intelligence activities, to legislative veto provisions. Furthermore, some of the proposals have included legislative authority over intelligence agencies for proposed committees in addition to oversight functions. Such proposals would necessarily remove legislative jurisdiction from other existing committees, whereas proposals which are exclusively oversight oriented would not do so, resulting instead in shared oversight jurisdiction with established standing committees. The focus here is on oversight functions, although the distinction between oversight and legislative functions can be obscure, especially when the former incorporates legislative veto provisions and/or authorizing authority regarding agencies.

The major themes of the current recommendations can be categorized as follows -- membership patterns, jurisdiction, authorizing authority, reporting requirements, legislative veto provisions, and disclosure of confidential or classified information.

One of the main issues involves membership patterns, specifically whether members should serve on a rotating basis or be selected and serve in a manner similar to other committees. Advocates of a rotating membership insist that this would preclude any small group of legislators from monopolizing intelligence oversight and information and from becoming captive clients

of the intelligence community. Opponents of rotation insist that the procedure would make security and confidentiality even more difficult to maintain, that it would contradict the principle of expertise developed by specialization, and that a by-product would be a stronger role for the staff vis-a-vis the legislators, since the former would serve continuously.

Jurisdictional differences abound because of different interpretations of what constitutes intelligence production and the requirements of congressional oversight. Oversight of foreign intelligence agencies dominates the recommendations but many recognize a need for surveillance over domestic agencies as well in order to provide comprehensive oversight. Some proposals focus on intelligence activities while others concentrate on the agencies themselves, and, thereby, might possess a more elaborate oversight responsibility.

Different recommendations involving authorizing authority relate to whether the proposed committees should authorize intelligence agency budgets or whether that power should remain with the existing standing committees.

Differences are also noticeable on the issue of reporting requirements. Several recommendations propose that the CIA report to the committee prior to embarking on clandestine non-intelligence operations, whereas others would require a report but without stipulating advanced notice, similar to the 1974 Foreign Assistance Act provision regarding notification of certain CIA non-intelligence activities to appropriate committees. 50/

50/ P. L. 93-559; 88 Stat. 1795. Discussion of this legislation is available in the section of the report dealing with current oversight of intelligence.

Legislative veto provisions have been advanced, specifically with regard to clandestine non-intelligence operations of the CIA. In essence, such provisions would permit the proposed committees to veto any particular CIA operation which meets that description within a specified time period. The legislative veto has been adopted in numerous pieces of legislation but its constitutionality has been questioned when a single committee (as opposed to the entire Congress) has authority to nullify an act of the executive branch. H. Lee Watson contends that the legislative veto, when held by a single committee, is unconstitutional because such a procedure bestows formal statutory powers on an individual committee, a power reserved for the entire congress. 51/ Others might contend that certain types of legislative vetoes are valid exercises of congressional power, even if excercised by single committees, in certain subject areas which are clearly sanctioned as congressional responsibilities by the Constitution, such as appropriations and executive departmental organization and reorganization. 52/

51/ H. Lee Watson, "Congress Steps Out: A Look at Congressional Control of the Executive," California Law Review, vol. 63 (July 1975), especially pp. 1045-1069.

52/ Examples of legislation incorporating the committee veto include Education Amendments of 1974, P. L. 93-380; 88 Stat. 484; the Public Buildings Act of 1959, P. L. 86-249; 73 Stat. 479; and Amendments to the National Traffic and Motor Vehicle Safety Act of 1966, P. L. 91-265, 84 Stat. 262. According to a survey of legislative veto provisions, the committee veto is the least used of the three types -- concurrent resolutions or veto power exercised by both chambers and resolutions by either house are more numerous than committee veto provisions. See Clark Norton, "Congressional Review, Deferral and Disapproval of Executive Actions: A Summary and an Inventory of Statutory Authority," Congressional Research Service report, Aug. 6, 1975, to be updated as a multilith, March, 1976. The War Powers Resolution (P. L. 93-148; 87 Stat. 555) is not directly relevant because it provides for approval processes by the full Congress, not a single committee, by concurrent resolution. As well the War Powers Resolution can be considered as imposing only "subsequent limitations" on Presidential actions,

In the case of intelligence agency activities, dispute exists about the degres of congressional involvement inherent in its constitutional powers vis-a-vis those of the President as commander-in-chief and as chief executive.

Supporters of the legislative veto exercised by a standing committee in the intelligence area would suggest that such a power is an inherent part of the authorizing and oversight responsibilities of the Congress, which are normally effected through the committee system. Moreover, because of the secrecy requirements surrounding intelligence operations, a committee veto procedure (as opposed to a full congressional veto or a single chamber veto power) would be the more appropriate vehicle to limit premature or unauthorized disclosure. Other practical considerations have produced disagreement. Proponents of the committee veto insist that the process can be expedited, when necessary, and that prior CIA consultation with a knowledgeable committee might preclude unnecessary, ineffective, and/or illegal or unconstitutional actions on the part of the Agency. Opponents suggest that delay would be an inevitable consequence of the consultation process, possibly negating the effectiveness of the proposed CIA operation, even if approved by the committee.

The final area of concern regarding a permanent standing committee on intelligence noted in the debates regards unauthorized disclosure of information. The sensitive, classified nature of intelligence production and operations demands controls over access to such information and its distribution. As noted in a previous section, information held by the Congress,

---

whereas the legislative veto provision advanced with regard to intelligence is a prior approval/disapproval requirement. For an interesting review of the War Powers Resolution and suggested modifications, see Michael J. Glennon, "Strengthening the War Powers Resolution: The Case for Purse-Strings Restrictions," Minnesota Law Review, vol. 60 (Nov. 1975).

even if confidential or classified, is under the control of that body; executive or judicial interference is minimal. Presently, the House has no enforcement provisions or sanctions regarding the release of such information by a Member, whereas Senate Rule 36.3 does provide relevant procedures for that chamber. The House Select Committee on Intelligence has approved a recommendation similar to the Senate rule that a House member who discloses without authorization classified information that jeopardizes the national security of the United States may be censured or expelled by two-thirds vote of the House.53/ This provision, which modifies House Rule 29, applies only to members and not to committee action, since the latter may be authorized to release classified or confidential information.

The present recommendations before the Congress regarding oversight of intelligence offer a variety of alternatives and represent many of the features which had been advanced in earlier reorganization efforts. The debates surrounding the proposals reflect the significance of oversight in general and of the intelligence in particular.

53/ Recommendation proposed by Rep. Otis Pike, chairman of the House Select Committee on Intelligence, which approved it by a vote of 11 to 2, Feb. 5, 1976.

WIRETAPPING AND ELECTRONIC SURVEILLANCE:
FEDERAL AND STATE STATUTES

TABLE OF CONTENTS

	Page
Preface	i
Introduction	1
Federal Law	23
State Law	36
Statutes	48
Federal	48
Alabama	82
Alaska	84
Arizona	88
Arkansas	93
California	94
Colorado	100
Connecticut	111
Delaware	120
District of Columbia	138
Florida	154
Georgia	165
Hawaii	171
Idaho	173
Illinois	174
Indiana	179
Iowa	180
Kansas	181
Kentucky	184
Louisiana	185

PREFACE

The main purpose of this paper is to compile the federal and state statutes relating to electronic surveillance (wiretapping and mechanical or electronic eavesdropping) in a single source. In order to facilitate the reader's use of these materials, we have included a brief history of the law in this area, with heavy emphasis on the decisions of the United States Supreme Court, brief summaries of federal and state law, and comparative charts indicating which states have enacted laws in this area. For those readers who may wish to do further research in this field, we have also included a selected bibliography of legal materials.

Introduction

Wiretapping, frequently assumed to be a twentieth century phenomenon, took place at least as early as the Civil War when tapping of enemy telegraph lines was fairly prevalent, Dash, Schwartz & Knowlton, The Eavesdroppers, 23(1959). The practice of tapping telegraph lines was not limited to cases of military intelligence and as a result a number of jurisdictions enacted statutes outlawing tapping. The statutes varied. Some simply prohibited wiretapping as such; others expanded existing laws which forbade telegraph employees from disclosing the contents of telegraph messages to cover all unauthorized disclosure; a third type merely amended statutes outlawing malicious mischief involving the property of telegraph and telephone companies. A substantial number of states enacted no statutes at all.

Although the first federal legislation was enacted during World War I, 40 Stat. 1017(1918), it was limited to the duration of the First World War and was clearly enacted to protect government secrets rather than individual privacy, see 56 Congressional Record 10761-765(1918).

The most frequently litigated wiretap cases involve the legality of law enforcement taps and the admissibility of resulting evidence. The United States Supreme Court first considered the question of admissibility of evidence obtained by wiretapping in Olmstead v. United States, 277 U. S. 438 (1928). Olmstead, a Seattle bootlegger, had been charged with conspiring to violate the National Prohibition Act and was convicted as a result of evidence secured from taps placed on his telephone by federal agents. Olmstead argued that his conviction should be reversed on the grounds that evidence so obtained was inadmissible because (1) the use of evidence secured by listening to his telephone conversations constituted an unreasonable search

and seizure in violation of the Fourth Amendment, (2) such evidence was a violation of his immunity from self-incrimination protected by the Fifth Amendment, and (3) wiretapping was prohibited by the law of the State of Washington where the taps occurred. His conviction was affirmed by the United States Court of Appeals, Olmstead v. United States, 19 F.2d 842 (9th Cir. 1927), and the United States Supreme Court, Olmstead v. United States, 277 U. S. 438 (1928). Chief Justice Taft, writing for the majority, rejected Olmstead's contentions:

> There is no room in the present case for applying the Fifth Amendment unless the Fourth was first violated. There was no evidence of compulsion to induce the defendants to talk over their many telephones. They were continually and voluntarily transacting business without knowledge of the interception. Our consideration must be confined to the Fourth Amendment. Id. at 462.

No violation of the Fourth Amendment occurred because that would require "an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making seizure [or presumably for purposes of making a search]." Id. at 466. Since the evidence had not been obtained in violation of the Constitution, then the only basis for applying the exclusionary rule, the Court applied the common law rule permitting the admission of evidence even if it had been secured illegally.

Justice Holmes in his dissent tersely characterized the conduct of federal officials as "dirty business." Id. at 470. Justice Brandeis questioned the majority's interpretation of the Fourth and Fifth Amendments. In a strong dissent, frequently cited by opponents of wiretapping, he wrote:

> The protection guaranteed by Amendments is much broader in scope. They [the drafters of the Constitution] conferred, as against the Government, the right to be let alone--the most comprehensive of rights and the right most valued by civilized

> men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual whatever the means employed, must be deemed in violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth. Id. at 478-79.

Chief Justice Taft had observed, "Congress may of course protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation...." Id. at 465. Such legislation was introduced but never enacted, see, e.g., H.R. 5416, 71st Cong., 1st Sess. (1929); H.R. 9893, H.R. 5305, H.R. 23, 72d Cong., 1st Sess. (1931). In 1934, Congress amended the Radio Act of 1927 with the Federal Communications Act of 1934, section 605 of which prohibited the interception and divulgence of wire or radio communications, 48 Stat. 1064, 1103-104 (1934).*

---

* No person receiving or assisting in receiving, or transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, to any person other than the addressee, his agent, or attorney, or to a person employed or authorized to forward such communications to its destination, or to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, or to the master of a ship under whom he is serving, or in response to a subpena issued by a court of competent jurisdiction, or on demand of other lawful authority; and no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person; and no person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by wire or radio and use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto; and no person having received such intercepted communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or any part thereof, knowing that such information was so obtained, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of the same or any part thereof, or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto: Provided, that this section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication broadcast, or transmitted by amateurs or others for the use of the general public, or relating to ships in distress. 48 Stat. 1064, 1103-104 (1934); 47 U.S.C. §605 (1940).

In Nardone v. United States, 302 U. S. 379 (1937), the Government argued that section 605 could not be interpreted as either a prohibition against governmental tapping or a restriction of the admissibility of evidence so obtained, since Congress had had opportunities to enact legislation which expressly overruled Olmstead and had chosen not to do so. The Court held that: "[T]he plain words of section 605 forbid anyone, unless authorized by the sender, to intercept a telephone message, and direct in equally clear language that 'no person' shall divulge or publish the message or its substance to 'any person.' To recite the contents of the message in testimony before a court is to divulge the message." Id. at 382 (emphasis of the Court). The defendants whose conversations had been reversed in Nardone were retried and convicted. They appealed on the grounds that they should have been permitted an opportunity to determine whether the evidence used against them was the product of the illegal wiretap. The United States Court of Appeals held that "Congress had not also made incompetent testimony which had become accessible by the use of unlawful 'taps', for to divulge that information was not to divulge an intercepted telephone talk." United States v. Nardone, 106 F. 2d 41, 44 (2d Cir. 1939). The Supreme Court reversed because affirming the conviction would result indirectly in the conduct which had been directly forbidden. The Court noted further:

> Sophisticated argument may prove a causal connection between information obtained through illicit wire-tapping and the Government's proof. As a matter of good sense, however, such connection may have become so attenuated as to dissipate the taint. A sensible way of dealing with such a situation -- fair to the intendment of §605, but fair also to the purposes of the criminal law -- ought to be within the reach of experienced trial judges. The burden is, of course, on the accused in the first instance to prove to the trial court's satisfaction that wire-tapping was unlawfully employed. Once that is established -- as was plainly done here -- the trial judge must give opportunity, however closely confined, to the accused to prove

> that a substantial portion of the case against him was a fruit of the poisonous tree. This leaves ample opportunity to the Government to convince the trial court that its proof had an independent origin. Id. at 341.

On the same day the second Nardone opinion was handed down, the Supreme Court read its decision in Weiss v. United States, 308 U. S. 321 (1939). Weiss was indicted with several others for mail fraud. Several government witnesses agreed to testify after hearing recordings of tapped telephone conversations between themselves and Weiss. At Weiss's trial, these witnesses testified as to the conversations and transcripts and records of the intercepted calls were admitted into evidence. Weiss was convicted, and his conviction affirmed by the Court of Appeals, United States v. Weiss, 103 F. 2d 348 (2d Cir. 1939). In response to Weiss's contention that his conviction should be overturned on the basis of section 605, the Government argued that section 605 had not been violated since, (1) the telephone conversations in question were intrastate and (2) the witnesses, parties to the conversations, had consented to divulge their contents subsequent to interception but prior to the divulgence at trial. The Court rejected the first on the basis of the language of the statute and the second because divulgence to Government agents and the United States Attorney had occurred prior to any consent of the parties whose conversations were intercepted.

In a subsequent case involving those indicted with Weiss, it was argued, that the testimony encouraged by showing the potential witnesses transcripts of their incriminating telephone conversations should be excluded. This was urged although the defendants were not parties to the intercepted conversations shown the witnesses. The Court affirmed, noting that although the use made of the intercepted conversations was in violation of

section 605, the resulting testimony was not thereby inadmissible against a person not a party to the conversation, Goldstein v. United States, 316 U. S. 114, 122 (1942).

In Goldman v. United States, 316 U. S. 129 (1942), Government agents, using a detectaphone placed against the common wall of an adjoining office, intercepted the conversations of the petitioners in their office including statements made into the office's telephone receiver during telephone conversations. The Court refused to overturn Olmstead and held that the case involved neither a "communication" nor an "interception" within the meaning of section 605.

The Court also refused to overturn a state conviction based, in part, upon evidence in the form of recordings of the defendant's telephone conversations intercepted by state law enforcement officials in violation of section 605, because it felt that the language and legislative history did not support the contention that Congress intended the section to impose a rule of evidence upon state courts, Schwartz v. Texas, 344 U. S. 199 (1952). Consistent with this view, the Court upheld a federal district court's denial of injunctive relief to prevent state law enforcement officers from using wiretaps to obtain evidence for use in state criminal trials, Pugach v. Dollinger, 365 U. S. 458 (1961). However, it refused to permit federal courts to admit evidence secured in violation of section 605, even though the tap was conducted by state rather than federal officers, Benanti v. United States, 355 U. S. 96 (1957).

In Rathbun v. United States, 355 U. S. 107 (1957), the Court found no violation of section 605 where the police secured evidence by listening

in on a telephone conversation over a regularly used extension with the consent of one of the parties to the conversation:

> The clear inference is that one entitled to receive the communication may use it for his own benefit or have another use it for him. The communication itself is not privileged, and one party may not force the other to secrecy merely by using the telephone. Id. at 110.

During this period the courts distinguished between wiretapping, forbidden by section 605, and other forms of mechanical eavesdropping. Eavesdropping was a common law misdemeanor indictable as a nuisance which included habitually "listen[ing] under walls or windows or the eaves of a house to harken after discourse, and thereupon to frame slanderous and mischievous tales", 4 Blackstone, Commentaries 168 (New ed. 1813); see, 2 Wharton, Criminal Law and Procedure §827 (Anderson, ed. 1957); 1 Bishop Criminal Law §1122 (9th ed. 1923). Common law eavesdropping is still punishable in a few states, but it has never been clear whether the offense prohibited both human and mechanical presence and whether it placed any restrictions on police conduct. Other states enacted statutes which expressly prohibited the interception of communications by mechanical or electronic devices, but these appear to have been the exception rather than the rule.

Challenges to the admissibility of evidence secured by intercepting conversations before the Supreme Court were generally based on section 605 and the Fourth Amendment. Except for those cases involving the interception of telephone conversation claims based on section 605 were universally unsuccessful. However, over a period of thirty years the Court slowly withdrew from the Fourth Amendment view articulated by Chief Justice Taft in Olmstead. As noted earlier, the Court rejected Olmstead's Fourth Amendment arguments because there had been no search and seizure of

tangible property and there had been no physical invasion of property for purposes of making a search and seizure -- presumably of a person or some tangible property. The first case of electronic surveillance which did not involve wiretapping was Goldman v. United States, supra, where conversations had been intercepted by means of a detectaphone placed against the party wall of an adjoining office. The Court found the case indistinguishable from Olmstead on Fourth Amendment grounds and refused to overrule or reconsider Olmstead.

In On Lee v. United States, 343 U. S. 747 (1952), it was argued that the Fourth Amendment had been violated when a former employee engaged On Lee in an incriminating conversation at his place of business. On Lee's conversations were transmitted by means of a device hidden on the person of a former employee and overheard by a government agent who testitied at trial. On Lee contended that the informer's presence in his shop constituted a trespass because in transmitting their conversation, the informer "vitiated the consent and rendered his entry a trespass ab initio" and because the consent had been vitiated by the fact it had been secured fraudulently. Id. at 751-52. The Court held the "fictional" dimensions of the civil law of trespass did not correspond to the test concerning rights protected by the Fourth Amendment. "Only in the case of physical entry, either by force, ... by unwilling submission to authority ... or without any express or implied consent" would Fourth Amendment problems be raised and then only in the distinguishable case of illegal seizure of tangible property. Id. at 752-53.

Two years after On Lee, the Supreme Court seems to have begun its departure from the requirement articulated in Olmstead that only

tangible objects could be the subject of Fourth Amendment protections. In Irvine v. California, 347 U. S. 128 (1954), the Court refused to restrict state use of evidence obtained by the interception of nontelephonic conversations. Irvine's conviction in California state courts had been accomplished, in part, through the use of evidence secured when the police concealed a microphone in the wall of Irvine's home. The Court concluded with some apparent reluctance:

> That officers of the law would break and enter a home, secrete such a device, even in a bedroom, and listen to the conversation of the occupants for over a month would be almost incredible if it were admitted. Few police measures have come to our attention that more flagrantly, deliberately, and persistently violate the fundamental principle declared by the Fourth Amendment as a restriction on the Federal Government.... The decision in Wolf v. California, 338 U. S. 25, 27, for the first time established that the concept of due process found in the Fourth Amendment.
>
> But Wolf, for reasons set forth therein, declined to make the subsidiary procedural and evidentiary doctrines developed by the federal courts limitations on the states. On the contrary, it declared, "We hold, therefore, that in a prosecution in a State court, for a State crime, the Fourteenth Amendment does not forbid the admission of evidence obtained by an unreasonable search and seizure." 338 U. S. 25, 33.... That holding would seem to control here. 347 U. S. at 132-33.

Thus, without expressly announcing such a view, the Court seems to have concluded that a Fourth Amendment violation occurred when Irvine's conversations were intercepted after a trespass onto his private property, notwithstanding the fact that the trespass was made for the purpose of installing listening devices and not for the search or seizure of any tangible object.

The Court continued this approach in Silverman v. United States, 365 U. S. 505 (1961), where District of Columbia police officers had driven a "spike mike" into the party wall of an adjoining house and into one of the heating ducts in Silverman's house. The mike enabled officers to overhear

conversations throughout the house via the heating duct. The officers were permitted to testify as to the content of the conversations at the trial that resulted in Silverman's conviction. The Court overturned Silverman's conviction, but was unwilling to overrule Olmstead, Goldman, or On Lee which it felt were all characterized by both an "absence of a physical invasion of the petitioner's premises" in connection with the interception and a lack of "an actual intrusion into a constitutionally protected area".*

The concept of "intrusion into a constitutionally protected area" also provided part of the foundation for the Court decision in Lanza v. New York, 370 U. S. 139 (1963). Lanza had been convicted of legislative contempt when he refused to answer questions of a New York legislative committee that had a transcript of intercepted conversations between Lanza and his brother. The Court distinguished the facts from Silverman, noting that Lanza's intercepted conversations had taken place in jail, a place which "shares none of the attributes of privacy of a home, an automobile, an office, or a hotel room." Id. at 143.

The Court's apparent departure from Olmstead with respect to the question of whether intangibles could be the objects of Fourth Amendment protection when acquired subsequent to a physical intrusion into a constitutionally protected area brought something of a reiteration of the consent arguments raised in On Lee. In Lopez v. United States, 373 U. S. 427

---

*In Clinton v. Virginia, 377 U. S. 158 (1964), the Court in a per curiam opinion reaffirmed its views in Silverman in a case with similar but not identical facts. The Court's earlier decision in Mapp v. Ohio, 367 U. S. 643 (1961), holding that the exclusionary rule and the Due Process Clause of the Fourteenth Amendment rendered inadmissible in a state criminal proceeding evidence secured in violation of the Fourth Amendment, enabled the Court in Clinton to avoid the result reached in Irvine v. California, supra.

(1963), a witness had surreptitiously recorded incriminating statements by the petitioner. Lopez contended, among other things that the recording of his attempts to bribe an Internal Revenue agent constituted an illegal search and seizure in violation of the Fourth Amendment since the agent misrepresented his willingness to accept the bribe. The Court rejected this argument, saying:

> Stripped to its essentials, petitioner's argument amounts to saying that he has a constitutional right to rely on possible flaws in the agent's memory, or to challenge the agent's credibility without being beset by corroborating evidence that is not suspectible of impeachment. For no other argument can justify excluding an accurate version of a conversation that the agent could testify to from memory. We think the risk that petitioner took in offering a bribe to Davis fairly excluded the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording. Id. at 439.

Justice Brennan wrote a strongly worded dissent urging repudiation of Olmstead and that "the procedure of antecedent justification before a magistrate that is central to the Fourth Amendment... be made a precondition of lawful electronic surveillance." Id. at 464 (Brennan, J., dissenting). *

Three years later in Osborn v. United States, 395 U. S. 323 (1966), the Court was presented with a case in which the government had attempted to comply with both the majority and dissenting opinions in Lopez. Osborn, an attorney, employed Robert Vick to investigate the prospective jurors for a federal criminal case. Vick was working at the same time with federal

---

*The problems raised by interception with the knowledge of only one party to the conversation were avoided in Massiah v. United States, 377 U. S. 206 (1964), where the Court held that the use of a government agent to elicit conversations which were surreptitiously transmitted to another federal agent was a violation of the Fifth and Sixth Amendments.

authorities, reporting to them "any illegal activities." When Vick reported a request by Osborn to have him influence one of the prospective jurors, government attorneys requested and received permission from two federal district court judges to conceal a recorder on Vick to verify the statements in his affidavit. The recordings were subsequently admitted into evidence at the trial which resulted in Osborn's conviction. The Court noted the questions raised on appeal had already been resolved by a majority of the Court in Lopez when it refused to condemn "the use by one party of a device to make an accurate record of a conversation about which the party later testified." 385 U. S. at 327. However, the Court went on to point out that admission was also consistent with the views expressed by the dissenters in Lopez.

The Court's withdrawal from the principles articulated in Olmstead became even more apparent in Berger v. New York, 388 U. S. 41 (1967) and Katz v. United States, 389 U. S. 347 (1967). Berger had been convicted of conspiring to bribe the Chairman of the New York State Liquor Authority on the basis of evidence obtained by eavesdropping authorized by a court order. It was held that the procedure established by the New York statute resulted in a blanket right to eavesdrop without the necessary judicial supervision or protection, thereby violating the Fourth Amendment guarantees against unreasonable searches and seizures made applicable to the states through the Due Process Clause of the Fourteenth Amendment.

Writing for the majority, Justice Clark noted with approval, the safeguards used by the Government in Osborn:

> Among other safeguards, the order described the type of conversation sought with particularity, thus, indicating the specific objective of the Government in entering the constitutionally protected area and the limitations placed upon the

> officer executing the warrant. Under it, the officer could not search unauthorized areas; likewise, once the property sought, and for which the order was issued, was found the officer could not use the order as a passkey to further search. In addition, the order authorized one limited intrusion rather than a series or a continuous surveillance. And, we note that a new order was issued when the officer sought to resume the search and probable cause was shown for the succeeding one. Moreover, the order was executed by the officer with dispatch, not over a prolonged and extended period. In this manner, no greater invasion of privacy was permitted than was necessary under the circumstances. Finally, the officer was required to and did make a return on the order showing how it was executed and what was seized. 388 U. S. at 56-57.

In contrast to the protections set forth in Osborn, the New York statute, N. Y. Code of Crim. Pro. §813-a: (1) failed to require description with particularity of the place to be searched and the person or thing to be seized, (2) failed to require a description with particularity of the crime that had been or was being committed, (3) failed to require a description with particularity of the type of conversation to be seized, (4) failed to place any limitations on the officer executing the order which would prevent his searching unauthorized areas, and prevent his searching further once the object of the search had been seized, (6) failed to require dispatch in executing the order, (7) failed to require that the officer to whom the order was issued return to the issuing court and show what had been seized, and (8) failed to require a showing of exigent circumstances to overcome the defect of not giving prior notice to those whose privacy had been invaded.

In Katz v. United States, 389 U. S. 347 (1967), the defendant was convicted of transmitting wagering information by telephone. His conviction was based in part upon evidence obtained by placing an electronic listening and recording device immediately outside the public telephone booth from which Katz placed his calls. Katz maintained that the govern-

ment had violated his Fourth Amendment rights by penetrating a "constitutionally protected area" and that the fruits of that violation should not have been admitted into evidence against him in his criminal trial. The Government contended that the Court need not reach the question of whether the conduct of its agents complied with Fourth Amendment requirements since the listening device had not intruded into a "constitutionally protected area." The Court was unwilling to consider the question in these terms and concluded:

> The Government contends, however, that the activities of its agents in this case should not be tested by Fourth Amendments requirements, for the surveillance technique they employed involved no physical penetration of the telephone booth from which the petitioner placed his calls. It is true that the absence of such penetration was at one time thought to foreclose further Fourth Amendment inquiry, Olmstead v. United States, 277 U. S. 438, 457, 464, 466; Goldman v. United States, 316 U. S. 129, 134-146, for that Amendment was thought to limit only searches and seizures of tangible property. But "[t]he premise that property interests control the right of the Government to search and seize has been discredited." Warden v. Hayden, 387 U. S. 294, 304. Thus, although a closely divided Court supposed in Olmstead that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested. Indeed, we have expressly held that the the Fourth Amendment governs not only the seizure of tangible items, but extends as well to to the recording of oral statements, overheard without any "technical trespass under ... local property law." Silverman v. United States , 365 U. S. 505, 511. Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people -- and simply "areas" -- against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.
>
> We conclude that the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that

> the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance. 389 U. S. 352-53.

Having concluded that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection; ... what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected," and that Katz was entitled to that protection when he used the telephone booth, the Court held that the requirement of the Fourth Amendment had not been met, because the search and seizure had been conducted without a warrant.

In Katz, the Court "conclude[d] that the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling" in electronic surveillance cases. In Lee v. Florida, 392 U. S. 378 (1968), the Court considered the erosive effect of subsequent case law on some of its earlier decisions concerning the interception of telephone conversations in violation of section 605 of the Communications Act, 47 U. S. C. §605. In Lee, Orlando police subscribed to a telephone on Lee's party line for the express purpose of eavesdropping on his telephone conversations. Recordings of Lee's telephone conversations acquired by means of equipment attached to the police phone on Lee's party line were introduced at Lee's state criminal trial. The State of Florida argued that the Court's decisions in Rathbun and Schwartz suggested that (1) Lee's conversations had not been intercepted and divulged in violation of section 605 and (2) even if they had been, Schwartz held Congress had not intended section 605 as a rule of evidence made binding in state criminal proceedings. The Court overturned Lee's conviction. Lee was distinguishable from

Rathbun, the Court felt, because in Rathbun one of the parties to the telephone conversation had previously consented to the police's use of a regularly used extension to listen in, whereas in Lee, neither party had consented to the police eavesdropping on their telephone conversations through the use of a party-line phone installed just for that purpose. Schwartz was overruled primarily because the Court felt that the principles upon which Schwartz was founded had been repudiated. In the Court's view, the Schwartz decision was based on two convictions and a hope. First, it evidenced a narrow interpretation of section 605; second, it expressed a belief that without express provision, state courts were free to accept or reject evidence secured in violation of federal law, statutory or constitutional; finally, it articulated the hope that enforcement of section 605 could be accomplished by criminal sanctions. The Court in Lee accepted none of these:

> The fact that a state official would be violating the express terms of the federal statute by the very act of divulging the intercepted communications as evidence for the prosecution at the trial, the Court in Schwartz said, was "simply an additional factor for a state to consider in formulating a rule of evidence for use in its own courts." Ibid. But in Benanti v. United States, 355 U. S. 96, five years later, the Court returned to the teaching of Nardone in giving emphatic recognition to the language of the statute that itself makes illegal the divulgence of intercepted communications. In Benanti, the Court held inadmissible, in a federal trial, communications that had been intercepted by state officers. "Section 605," the Court said, "contains an express, absolute prohibition against the divulgence of intercepted communications." 355 U. S., at 102.
>
> After the Benanti decision, therefore, the only remaining support for Schwartz v. Texas, supra, was the holding Wolf v. Colorado, supra, that state courts, unlike federal courts, were free to decide for themselves whether to condone violations of federal law by accepting the products of such violations as evidence. That doctrinal underpinning of the Schwartz decision was, of course, completely removed by Mapp v. Ohio, 367 U . S. 643, which overruled Wolf and

> squarely held that evidence obtained by state officers in an unreasonable search is inadmissible in a state criminal trial.
>
> Finally, our decision today is counseled by experience. The hope was expressed in Schwartz v. Texas that "[e]nforcement of the statutory prohibition in §605 can be achieved under the penal provisions" of the Communications Act. 344 U. S., at 201. That has proved to be a vain hope. 392 U. S. at 384-85, 386.

The Supreme Court subsequently held that Berger, Katz, and Lee should be applied only prospectively, Kaiser v. New York, 394 U. S. 280 (1969); Desist v. United States, 394 U. S. 244 (1969); Fuller v. Alaska, 393 U. S. 80 (1969).

In Alderman v. United States, 394 U. S. 165 (1969), the opinion of the Court, written by Mr. Justice White, held that where the Government had conducted electronic surveillance in violation of the Fourth Amendment those who have standing, i.e., those whose conversations were intercepted and those whose premises had been invaded to conduct the surveillance, were entitled to suppression of any evidence so obtained. Once standing and unlawful electronic surveillance had been established, Justice White wrote, the determination of whether any of the intercepted conversations provided the Government with evidence which could not be used against defendants with standing could not be made either ex parte by the Department of Justice or by the trial court after an in camera inspection of the surveillance records. However, the right to inspect the surveillance records could be accompanied by a court order prohibiting unwarranted disclosure and could encompass only the right to inspect records of the intercepted conversations and the examination of "appropriate officials" to determine the extent to which they had been used in preparing the Govern-

ment's case.[1] Of course, where the interception was lawful, the Alderman safeguards do not apply, Giordano v. United States, 394 U. S. 310 (1969), and they can only be relied on by those with standing, Taglianetti v. United States, 394 U. S. 316 (1969).

After the Court's decision in Katz, the lower federal courts were divided on the question of the continued vitality of On Lee. The United States Court of Appeals for the Seventh Circuit held:

> It is our opinion, however, that the surreptitious placing of the key set on informer Jackson was for all conceptual purposes the same as the surreptitious wiring of the telephone booth in Katz. Each was part of a "bugging" technique by which a conversation was transmitted to an "uninvited ear" -- government agents. The crucial fact in each case is that the respective speakers did not consent to the overhearing of their statements and that the conversations were overheard by third persons uninvited by the speaker.
>
> To claim, as the Government does, that one party can waive the fourth amendment rights of another, is the same thing as saying that Katz would have been decided differently if the recipient of the intercepted phone call had consented

---

[1] Alderman is complicated by the fact that it involves three cases, Alderman where the Government was moving for a modification of the Court's order in Kolod v. United States, 390 U. S. 136 (1968), in which the determination of whether intercepted conversations had provided evidence against petitioners was remanded to the trial court for decision following an adversary hearing, and Ivanov v. United States and Butenko v. United States, "national security" cases before the Courts on grants of certiorari. Justice White wrote the opinion of the Court, joined by Chief Justice Warren and Justice Brennan. Justice Black dissented on the basis of his dissent in Katz. Justice Marshall took no part in consideration or decision of the case. Justice Harlan concurred in part and dissented in part, noting that he would limit standing to those whose conversations were intercepted and would permit in camera inspection in cases with special circumstances such as the "national security" aspects of Ivanov and Butenko. Justice Stewart concurred in Justice Harlan's opinion, except that he would not permit in camera in the Ivanov and Butenko cases. Justice Fortas filed an opinion concurring in part and dissenting in part in which he would have recognized standing in any subject of the investigation in which electronic surveillance was used unlawfully and would have permitted in camera inspection of "information vital to national security... to determine its relevance or materiality...." Justice Douglas joined the opinion of the Court but concurred in that part of Justice Fortas' opinion dealing with standing.

> to the Government's bugging. We are unable to believe that such a meaningless form of consent would have rendered the defendant's overheard statements any more admissible in Katz.
>
> The most lethal blow to On Lee was dealt by the Court's overruling in Katz of the Goldman and Olmstead bulwark which provided the conceptual basis for On Lee. The overruling of these cases, combined with the reasoning of Katz, leaves no scope for On Lee's teaching. United States v. White, 405 F. 2d 838, 843, 847-48 (7th Cir. 1969).

The Supreme Court disagreed, noting that Katz had left intact convictions based upon evidence acquired when the defendant voluntarily confided in one who revealed the conversation, Hoffa v. United States, 385 U. S. 293, 302 (1966), or in one who recorded the conversation, Lopez v. United States, 373 U. S. 427 (1963), or in one who was later revealed to be a government agent sent to gather information concerning narcotics, Lewis v. United States, 385 U. S. 206 (1966). The Court refused to distinguish between the case of conversations seized by a government agent participating in a conversation and utilizing a recording device and the case of a government agent's taking part in a conversation and transmitting it for another to record. The Court felt further, that the Seventh Circuit was also in error, because the interception in White occurred before the Katz decision; therefore, the law in effect prior to Katz, including On Lee, should have been applied as required by Desist.

Two of the preceeding cases, Katz and Berger, were largely responsible for much of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 197; 18 U.S.C. §§2510-2520, see United States v. United States District Court for the Eastern District of Michigan, 407 U. S. 297, 302 (1972). In Katz, the Court observed:

> They [the Government agents] did not begin their electronic surveillance until investigation of the petitioner's activities

> had established a strong probability that he was using the telephone in question to transmit gambling information to persons in other states, in violation of federal law. Moreover, the surveillance was limited, both in scope and in duration, to the specific purpose of establishing the contents of the petitioner's unlawful telephonic communications. The agents confined their surveillance to the brief periods during which he used the telephone booth and they took great care to overhear only the conversations of the petitioner himself.
>
> Accepting this account of the Government's actions as accurate, it is clear that this surveillance was so narrowly circumscribed that a duly authorized magistrate, properly notified of the need for such investigation, specifically informed of the basis on which it was to proceed, and clearly apprised of the precise intrusion it would entail, could constitutionally have authorized, with appropriate safeguards, the very limited search and seizure that the Government asserts in fact took place. 389 U. S. at 354.

Yet Berger and Katz had created some doubt as to the extent to which law enforcement officials might use wiretapping and electronic surveillance at a time when there were increasing assertions of its utility as a law enforcement tool. The President's Commission Law Enforcement and Administration of Justice noted:

> Over the years New York has faced one of the Nation's most aggravated organized crime problems. Only in New York have law enforcement officials achieved some level of continuous success in bringing prosecutions against organized crime. For over twenty years, New York has authorized wiretapping on court order. Since 1957, "bugging" has been similarly authorized. Wiretapping was the mainstay of the New York attack against organized crime until Federal court decisions intervened. President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society, 201 (1967).

Congress was aware of this concern. It was also aware of the vacillating protection granted under state and federal law against the wiretapping and electronic surveillance conducted for purposes other than law enforcement. Title III was the product of these concerns. It attempted to protect individual privacy while providing law enforcement agencies with a judicially supervised procedure authorizing the interception of wire and

oral communications consistent with the constitutional restrictions enunciated by the courts.

In United States v. United States District Court for the Eastern District of Michigan, 407 U. S. 297 (1972), the three defendants were indicted on charges growing out of the destruction of an office of the Central Intelligence Agency in Ann Arbor, Michigan. The Government contended that 18 U.S.C. §2411(3)* constituted congressional recognition or affirmance of a constitutional authority in the President to conduct warrantless domestic security surveillance involving purely domestic threats to national security. The Government had engaged in warrantless eavesdropping "to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." 407 U. S. at 300. The conversations of one of the defendants had been intercepted. Over the Government's contention that the interception was a reasonable exercise of the President's power to protect the national security, the United States District Court for the Eastern

---

*Section 2511(3) of Title 18 of the United States Code provides:

Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605), shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take measures as he deems to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial, hearing, or other proceeding, only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

District of Michigan held that the interception violated the Fourth Amendment and ordered the Government to permit the defendant to examine the content of the intercepted conversations. The United States Court of Appeals denied the Government's petitition for a writ of mandamus requiring the District Court to set aside its order, United States v. United States Court for the Eastern District of Michigan, 444 F. 2d 651 (6th Cir. 1971).

The Supreme Court affirmed, concluding that 18 U.S.C. §2511(3) "simply left presidential powers where it found them." 407 U. S. at 303. The Court did not feel that the President's constitutional powers included the authority to permit interception of the conversations in cases of purely domestic threats to national security without regard for the restrictions of the Fourth Amendment, particularly the warrant clause. While Justice Powell, writing for the Court, indicated that standards other than those set forth in Title III -- 18 U.S.C. §2518 -- for traditional types of criminal activity might be compatible with the Fourth Amendment in national security cases, he held that "prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe. "407 U. S. at 324. The Court noted the special nature of this category of cases, saying:

> Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillance to oversee political dissent. Id. at 320.

In Gelbard v. United States, 408 U. S. 41 (1972), the Court concluded that a witness held in civil contempt for refusing to testify before a federal grand jury could invoke 18 U.S.C. §2515 as a defense where the

questions before the grand jury were based upon an illegal interception of wire or oral communications.

In United States v. Kahn, 415 U. S. _____ (1974), the Court held that the provisions of Title III requiring the identification of persons whose communications are to be intercepted, "if known", 18 U. S. C. §§2518(1)(b)(iv), 2518(4)(a), referred to one whom the law enforcement officials seeking the order had probable cause to believe was committing an offense and not one whose identity was known but whose criminal involvement was unsuspected.

Title III permits application for interception orders and extensions when authorized by "the Attorney General, or any Assistant Attorney General specially designated by the Attorney General." 18 U.S.C. §2516(1). The statute does not permit applications initially authorized by the Attorney General's Executive Assistant and evidence obtained as the result of an order issued on such an application or as the result of an extension to such an order is inadmissible under Title III, 18 U.S.C. 2515, United States v. Giordano, ____ U.S. ____ (1974). However, identification of an Assistant General as the authorizing officer when in fact application was authorized by the Attorney General does not invalidate the interception order granted on the application, United States v. Chavez, ____ U.S. ___(1974).

FEDERAL LAW

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 197, 211 (1968), as amended, 18 U.S.C. §§2510-2520, represents an attempt to reconcile the interests of individual privacy with the needs of law enforcement. Title III is not universal in its coverage. The Title, as amended, does not prohibit the following: (a) communication carrier

employees intercepting, disclosing or using wire communications during the normal performance of their duties or to assisting law enforcement officials acting under the authority of 18 U.S.C. §§2510-2520; (b) Federal Communications Commission employees intercepting communications during the the performance of their duties in enforcing chapter 5 of title 47 of the United States Code; (c) anyone acting under color of law intercepting communications with the consent of one of the parties to the communication with the consent of one of the parties to the communication; (d) anyone acting with the consent of one of the parties to the communication intercepting communications as long as the purpose of the interception is not tortious, criminal or injurious; and (e) those intercepting communications under judicial authorization, 18 U.S.C. §2511(1),(2). The Title also states that it is not to be construed as a limitation upon the constitutional authority of the President to protect national security, 18 U.S.C. §2511(3). Moreover, the oral communications protected are limited by definition to those "uttered by a person exibiting an expectation that such communication is not subject to interception under circumstances justifying such expectations" 18 U.S.C. §2510(2); see, Katz v. United States, supra at 351-52; Id. at 361 (Harlan, J., concurring). Finally, subsection (1) of 18 U.S.C. §2511 suggests that there may be a jurisdictional limitation on crimes defined in that section. Section 2511(1)(a) prohibits the interception of all wire or oral

communications by use of a mechanical device.* Subsection 2511(1)(b), on the other hand, prohibits the interception of oral communications by use of a mechanical device only under more limited jurisdictional circumstances, i.e., where (i) the device involves wire, cable or radio components, (ii) transmits or interferes with the transmission of radio communications, (iii) the device or one of its components is known to have been mailed or transported in interstate commerce, (iv) interception involves a business which affects interstate or foreign commerce, or (v) the conduct occurs in the District of Columbia, Puerto Rico, or any territory of the United States. This apparent duplication stemmed from congressional concern with the constitutionality of section 2511(1)(a). Summarizing this feeling, the Report of the Senate Committee on the Judiciary stated:

> Although the broad prohibitions of subparagraph (a) could, for example, be constitutionally applied to the unlawful interception of oral communications by persons acting under the color of State or Federal law, see Katzenbach v. Morgan, 384 U. S. 641 (1966), the application of the paragraph to other

---

*Strictly speaking, 18 U.S.C. §2511(1)(a) and (1)(b) prohibit interception, endeavoring to intercept, or procuring another to intercept or endeavor to intercept; subsections 2511(1)(c) and (d) prohibit knowing, willful disclosure or use or endeavors to disclose or use of the contents of communications intercepted in violation of subsection (1)(a) or (1)(b). For purposes of 18 U.S.C. §§2510-2520, "intercept" is defined as "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device, 18 U.S.C. §2510(4), and "electronic, mechanical, or other device" as "any device or apparatus which can be used to intercept a wire or oral communication other than -- (a) any telephone or telephone instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal." 18 U.S.C. §2510(5).

> circumstances could in some cases lead to a constitutional challenge that can be avoided by a clear statutory specification of an alternative constitutional basis for the prohibition. S. Rep. No. 1097, 90th Cong., 2d Sess. 92 (1968).

Subject to these restrictions, it is a federal crime to: (1) intercept, attempt to intercept or procure someone else to intercept or attempt to intercept any wire or oral communication, 18 U.S.C. §§2511(1)(a), and (1)(b), (2) disclose or attempt to disclose information obtained by unlawful interception, 18 U.S.C. §2511(1)(c); (3) use or attempt to use information obtained by unlawful interception, 18 U.S.C. §2511(1)(d); (4) mail, or send or carry in interstate or foreign commerce, any device primarily useful for the purpose of surreptitious interception, 18 U.S.C. §2512(1)(a); (5) manufacture, assemble, possess, or sell such a device which has or will be mailed or transported in interstate or foreign commerce, 18 U.S.C. §2512(1)(b); or (6) advertise such a device or what purports to be such a device, knowing that the advertisement will be mailed or transported in interstate or foreign commerce, 18 U.S.C. §2512(1)(c). Government employees, employees of a communications carrier and those under contract to a communications carrier or governmental agency are exempt from the prohibitions of section 2512, 18 U.S.C. §2512(2). Any devices used in violations of these sections may be confiscated, 18 U.S.C. §2513; see also, 28 C.F.R. §§8.1, 8.2 (1973). The contents of an illegally intercepted wire or oral communication may not be used directly or indirectly in any state or federal legal proceeding, 18 U.S.C. §2515; see also, Gelbard v. United States, 408 U. S. 41 (1972). Violations of these provisions may result in both civil and criminal penalties and those whose conversations are unlawfully intercepted, disclosed or used may recover statutory and punitive damages, reasonable attorney's fees, and other reasonable costs of recovery.

18 U.S.C. §2520. A good faith reliance in judicial or legislative authorization to engage in the interception of wire or oral communications is a complete defense to civil or criminal liability, Id.

Title III also amended section 605 of the Federal Communications Act which had prohibited the interception and disclosure of wire and radio communications. As amended, and subject to the authorizations of 18 U.S.C. §§2510-2520, the amended version of section 605 is limited primarily to the interception of radio communications and those transmitting or receiving, or assisting in receipt or transmission, of wire or radio communications in interstate or foreign commerce, 47 U.S.C. §605.

Perhaps the most controversial sections of Title III are those permitting law enforcement officials to secure a court order approving the interception of oral and wire communications, 18 U.S.C. §§2516-2519. The procedure whereby law enforcement agencies may secure the court order necessary to institute a wiretap or other form of electronic surveillance is rather detailed. Any Federal judge of competent jurisdiction, as defined by 18 U.S.C. §2510(9), may authorize the FBI or any other Federal investigative agency to intercept wire or oral communications upon the application of the Attorney General or any Assistant Attorney General designated by the Attorney General. State court judges of competent jurisdiction may issue a similar order upon the application of the principal prosecuting attorney of the state or any of its political subdivisions, providing state law authorizes the judge to issue such an order and providing that the order is granted and executed in compliance with the requirements of Title III and

state law.* Federal interceptions may be conducted only for the purposes of producing evidence of any of a number of specifically designated crimes ranging from murder and treason to bankruptcy fraud, 18 U.S.C. §2516(1). State orders are permitted where the interception may produce evidence of the commission of a "crime dangerous to life, limb or property and punishable by imprisonment for more than one year," or one of a list of specifically enumerated offenses, 18 U.S.C. §2516(2).

Every order must fulfill specific requirements involving statements made in the application which preceeded its issuance, the criterion used by the court in issuing the order, and the narrow scope of the order. Every application must be in writing, under oath, and contain a statement indicating: (1) the applicant's authority to request the order; (2) the identities of the applicant, of the official who authorized his application, and of the person who committed the offense under investigation and whose conversations are being intercepted, if the name of such person is known, see United States v. Kahn, 415 U. S. ____(1974); United States v. Giordano, ____ U.S. ___ (1974); United States v. Chavez, ___ U.S. ___ (1974); (3) a full and complete statement of the facts justifying the issuance of an order including details of the particular offense involved, a particular description of the facilities to be tapped or of the place where the oral communications are to be intercepted and of the type of conversation sought and whether alternative investigative methods have proved or are likely to prove either too dangerous

---

*While state court judges may issue search warrants to federal law enforcement officials, Fed. Rules of Crim. Pro., Rule 41(a), it is clear, that under 18 U.S.C. §§2510-2520, federal law enforcement officials seeking approval to intercept wire or oral communications, may only obtain orders from a federal judge and state officers only from state judges of competent jurisdiction, 18 U.S.C. §2516.

or unproductive; (4) the period of time for which the interception must be maintained; (5) if the interception is to continue after the conversations specified in the application have been secured, the statement must indicate facts establishing probable cause to believe that additional commmunications of the same type will occur; (6) a complete summary of all prior applications involving the same persons, facilities or places; and (7) where the application is for an extension of an existing order, there must be a statement of the results thus far obtained or reasons for the failure to obtain results, 18 U.S.C. §2518.

Before granting such an order, the court must be convinced that there is probable cause to believe that one of the offenses listed in 18 U.S.C. §2516 or the appropriate state statute is, has been, or is about to be committed; that there is probable cause to believe that communications involving the offense will be secured by the proposed interception; that alternative methods of investigation have proved or are likely to prove to be too dangerous or unproductive; and that there is probable cause to believe that the facilities being tapped or the place where the interception is to take place are either involved in the commission of the offense or leased, listed or commonly used by the person designated in the application, 18 U.S.C. §2518.

Every order must state the identity of the person whose conversations are to be intercepted, if known, see, United States v Kahn, supra; the facilities or place where the interception is to take place; a particular description of the type of conversation sought and the offense(s) involved; the identity of the agency empowered to conduct the interception and the official who authorized the application; and the period of time during which the interception is authorized, 18 U.S.C. §2518.

No order or extension is effective for longer than is required to secure the commmunications specified in the order or in any event for longer than thirty days without an extension, Id. Applications for the granting of extensions are subject to the same requirements imposed in the original order, Id.

The court, in the exercise of its discretion, may require additional evidence to justify the issuance of any order and reports as to the result of the authorization after the order has been issued, Id.

Section 2518 of title 18 also contains a provision which allows interception by law enforcement officials without a court order approving their conduct. Under subsection (7):

> [A]n investigative or law enforcement officer, specially designated by the Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, or who reasonably determines that -- (a) an emergency situation exists with respect to conspiratorial activities threatening the national security or to conspiratorial activities characteristic of organized crime that requires a wire or oral communication to be intercepted before an order authorizing such interception can with due diligence be obtained, and (b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire or oral communications if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur....

Such interceptions must end when an application for an order is denied or when the communication sought has been obtained, unless an order is granted. Id.

Where possible, intercepted conversations must be recorded in such a way as to preclude alteration and the recordings made available upon final termination to the judge who issued the order, 18 U.S.C. §2518.

Absent a showing of good cause for postponement, persons named in the order or application and any other parties to the intercepted conversations whom the court feels should be notified must be informed of the existence of the order or application, the date of its entry or denial, the period of time during which the interception was approved, and whether any communications were intercepted, Id. This notification must be given within ninety days after the final termination of an order or after a denial of an application, following interception authorized under 18 U.S.C. §2518(7). The court may make portions of the intercepted communications available to the person or his attorney for inspection as the interests of justice require, 18 U.S.C. §2518.

The Administrative Office of the United States Courts is required to publish annual reports summarizing the information state and federal judges must furnish in connection with receipt of requests to approve interceptions, 18 U.S.C. §2519.

Congress has authorized the creation of two commissions to study the effects of wiretapping and other forms of electronic surveillance by federal and state enforcement agencies. These commissions, the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance and the National Commission on Individual Rights, were established by the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 223, and the Organized Crime Control Act of 1970, 84 Stat, 960, respectively. The provisions authorizing creation of the Individual Rights Commission became effective January 1, 1972; those permitting establishment of the Wiretapping Commission on June 19, 1973. *

---

*At this writing only the Wiretapping Commission has been appointed.

This statement coupled with the fact that elsewhere in the Act when Congress did not intend to pre-empt state law, it expressly indicated that intention (see §902, 82 Stat. 234, 18 U.S.C. §927) suggests that Congress intended to establish a uniform federal law which would supersede nonconforming state law, except as provided for in the Act. However, the Senate Judiciary Committee in summarizing subsections 2511(1)(c) and 2511(1)(d), prohibiting the disclosure or use of information obtained by means of unlawful interception, and 2512, forbidding the manufacture, distribution, etc., of wiretapping and electronic eavesdropping devices state, "There is no intent to pre-empt State law." S. Rep. No. 1097, 90th Cong., 2d Sess. 93, 94 (1968). The report does not indicate whether subsections 2511(1)(a) and (b) outlawing interceptions were also intended to supplement rather than supersede state law.

Finally, there is the question of the status of state law in those areas which Title III excludes from coverage -- interception by or with the consent of one of the parties, and interception by the communications carrier or FCC employeess, for example. The Act merely states that these interceptions are not unlawful under Title III. Therefore, it is at least arguable that such interceptions would be governed by state law unless in conflict with or superseded by some other federal statute. This argument would seem to be even more persuasive, in view of the Supreme Court's interpretation of 18 U.S.C. §2511(3) in United States v. United States District Court, 407 U. S. 297, 301-308 (1972).

In any event, at present, a majority of the states have statutes prohibiting the interception of wire or oral communications. (See Table I). Most of these authorize judicially supervised law enforcement interception.

Courts of competent jurisdiction in each of these states are therefore permitted to issue warrants approving interceptions as long as the warrants and execution of the warrants complies with the requirements of the Title III as amended and any additional restrictions contained in state law. The Senate Report on Title III suggests that a state may exercise the authority to approve the interception of communications by its law enforcement officers only when it has a statute at least as demanding as the requirements of Title III, S. Rep. No. 1097, 90th Cong., 2d Sess. 98 (1968). This is not so. Section 2516(2) of title 18 of the United States Code merely requires that the state statute authorize the principal prosecuting attorney of the State or of any of its political subdivisions, to apply to a court of competent jurisdiction, for any order permitting interception. However, in issuing the order, the court must comply with the procedures of 18 U.S.C. §2518, and any additional requirements imposed by state statute. State wiretapping and electronic surveillance statutes are discussed more fully elsewhere in this report.

The Federal wiretapping and electronic surveillance policy contained in Title III has been augmented by a number of rules, regulations and internal memoranda issued by federal executive agencies. Some of these merely implement the provisions of Title III, e.g., 28 C.F.R. §§8.1, 8.2 covering the forfeiture procedures to be followed in seizing unlawful wiretapping and electronic eavesdropping equipment, cf., 18 U.S.C. §2513. Others deal with the extent to which personnel of a particular federal agency may engage in wiretapping and electronic surveillance, e.g., 32 C.F.R. §§42.1-42.8, restricting use by personnel of the Department of Defense; internal memoranda interceptions by personnel of various federal agencies

included in FCC Monitoring of Employees' Telephones, H. R. Rep. No. 92-1632, 92d Cong., 2d Sess., 32-41 (1973).* However, there are several rules, regulations and internal memoranda of more general applicability. Perhaps the most basic of these are the memoranda of President Johnson and Attorney General Ramsey Clark. President Johnson's memorandum of June 30, 1965, to the heads of all executive departments and agencies commanded their adherence to the following guidelines:

> (1) No federal personnel is to intercept telephone conversations within the United States by mechanical or electronic device, without the consent of one of the parties involved. (except in connection with investigations related to the national security).
>
> (2) No interception shall be undertaken or continued without first obtaining the approval of the Attorney General.
>
> (3) All federal agencies shall immediately conform their practices and procedures to the provisions of this order. United States v. United States District Court, 444 F.2d 651, 671 (App. A), (6th Cir. 1971).

President Johnson's order was supplemented on June 16, 1967, by a similar memorandum of Attorney General Ramsey Clark. The Clark memorandum (1) reiterated the prohibition against federal personnel intercepting telephone conversations without the consent of one of the parties to the conversation, (2) required each agency to adopt rules governing interception where one of the parties had consented, (3) prohibited the interception of non-telephone conversations in violation of the Constitution or a statute, (4) established a system of controls for interception of non-telephone conversations by federal personnel which included a requirement that advance approval be obtained from the Attorney General and that an annual report be made to the Attorney General by federal agencies concerning their use

---

*Other than those regulations contained in the Code of Federal Regulations, the existence and continued validity of agency rules, regulations and internal memoranda can only be ascertained by contacting a particular agency.

of interception equipment. FCC Monitoring of Employees' Telephones, H.R. Rep. No. 92-1632, 92d Cong., 2d Sess. 63-66 (1973). The policy announced in these memoranda is apparently still in force, Id. at 63 (letter of Asst. Att. Gen. Petersen).

The regulations of the Federal Communications Commission, because of that agency's responsibilities in regulating the communications industry, are also of general applicability. There are several FCC provisions. Sections 2.701, 15.11 and 15.220, prohibit eavesdropping by means of a radio device without the consent of all parties to the conversation; violation of these regulations is punishable by a fine of not more than $500 for each day of the violation, 47 U. S. C. §502. A regulated communications carrier (telephone company) may only record telephone conversations as long as a "beeper tone" is used during recording, 47 C.F.R. §64.501. However, the beeper tone is also part of the FCC's tariff requirements. * Since 1948, the FCC has required telephone companies to provide equipment that omits an audible beeper tone when connecting voice recording equipment with the facilities of the telephone company, 11 F.C.C. 1033 (1947); 12 F.C.C. 10005 (1948); 12 F.C.C. 10008 (1948). The FCC provisions apply only to "the use of recording devices in connection with interstate and foreign message toll telephone service" but "similar tariff regulations applicable to the use of recording devices in connection with local and intrastate telephone service have been filed by the telephone companies with respective

---

* Black's Law Dictionary defines tariff as "A cartel of commerce, a book of rates, a table or catalogue, drawn usually in alphabetical order, containing the names of several kinds of merchandise, with the duties or customs to be paid for the same, as settled by authority, or agreed on between the several princes and states that hold commerce together...."

state regulatory commissions." FCC Public Notice 60591 (March 28, 1951); see also, ___F.C.C. 2d___(F.C.C. 72-1127) (Dec. 20, 1972), (exempting use of the beeper tone where the recorded converation is to be broadcast and the parties are aware of that fact).

STATE LAW

Although federal law is obviously applicable in each of the states, there are a number of state laws regulating wiretapping and electronic surveillance. These statutes fall into three basic categories: 1) prohibitions against wiretapping and/or electronic surveillance, 2) authorization for law enforcement personnel to engage in wiretapping and/or electronic surveillance under judicial supervision, and 3) civil remedies available to those who are the victims of unlawful wiretapping and/or electronic surveillance. A few states have no such statutes and in these jurisdictions regulation is strictly a matter of federal law.* Others have retained the malicious mischief statutes which prohibit only wiretapping, see discussion supra at 1 .** However, a growing majority have enacted legislation generally outlawing both wiretapping and electronic surveillance. Most of these are similar to federal statute, authorize interception under court order by law enforcement officials, and frequently include provisions on the availability of civil

---

*Some states recognize the common law offense of eavesdropping and while we have been unable to find any cases on point, it seems unlikely that such an offense would be construed to include mechanical or electronic surveillance.

**Several states have malicious mischief statutes making it a crime to cut or destroy telephone or telegraph company lines or equipment; however, the courts have consistently held these do not prohibit wiretapping unless specific language is included with the statute, State v. Nordskog, 76 Wash. 472, 136 P. 694 (1913); Young v. Young, 56 R.I. 401, 185 A. 901 (1936); State v. Tracey, 100 N.H. 267, 125 A. 2d 774 (1956).

relief for violations. However, most of the state statutes contain some highly individualistic characteristics and for this reason no attempt to summarize their provisions will be made other than the chart which follows.

CHAPTER IV

Federal Government Materials

Summary of Contents

A. Executive Branch

This chapter contains the following items:

U.S. Department of Justice. Criminal justice information systems. Federal register, v. 40, no. 98, May 20, 1975: 22114–22119.

U.S. Department of Justice. Guidelines for domestic security investigations, White House personnel security and background investigations, and reporting on civil disorders and demonstrations involving a Federal interest. March 10, 1976 (Washington, D.C.) 20 p.

U.S. Department of Justice. Memorandum for the Attorney General—Subject: Electronic Surveillance, and National Security Electronic Surveillance History, Policy and Procedure (Memoranda from William Olson to Elliot Richardson). U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure and Subcommittee on Constitutional Rights. Committee on Foreign Relations. Subcommittee on Surveillance. Warrantless wiretapping and electronic surveillance—1974. Joint hearings, 93d Congress, 2d session. April 3–May 23, 1974. pp. 18–39.

U.S. Department of Justice. Standards and procedures for reviewing requests for electronic surveillance. Attorney General Edward Levi. Letter to Senator Edward M. Kennedy expressing support of "The Foreign Intelligence Surveillance Act of 1976" (S. 3197), June 29, 1975. Source: U.S. Congress. Senate. Committee on the Judiciary. Foreign Intelligence Surveillance Act of 1976. Report (to accompany S. 3197). July 15, 1976. Senate Report no. 94–1035.

U.S. Federal Communications Commission. Memorandum on the use of telephone extension to monitor improper communications; Administrative Order no. 12 and letter from Dean Burch, Chairman, FCC, to John Moss, Chairman, House Committee on Government Operations. U.S. Congress. House. Committee on Interstate and Foreign Commerce. Special Subcommittee on Investigations. FCC monitoring of employees' telephones. Hearings, 92d Congress, 2d session. March 28 and May 16, 1972. pp. 48–52.

U.S. Internal Revenue Service. Inspection of returns by Federal agencies. U.S. Congress. House. Committee on Ways and Means. Subcommittee on Oversight. IRS operations and taxpayer assistance. Hearings, 94th Congress, 1st session. Feb. 27 and April 14, 1975. p. 72.

U.S. Internal Revenue Service. Inventory of mechanical and/or electronic devices in custody of the Intelligence Division and the Inspection Service's Internal Security Division. U.S. Congress. House. Committee on Government Operations. Subcommittee on Commerce, Consumer, and Monetary Affairs. Oversight hearings into the operations of the IRS. Hearings, 94th Congress, 1st session. May 14–July 31, 1975. pp. 415–416.

U.S. Office of Telecommunications Policy. Executive Office of the President. Cable (report to the President). Jan. 14, 1974 (Washington, D.C.).
U.S. Postal Service. Mail covers (statement by William J. Cotter, Chief Postal Inspector). U.S. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Postal Facilities, Mail, and Labor Management. Postal Inspection Service's monitoring and control of mail surveillance and mail cover programs. Hearings, 94th Congress, 1st session. May 6–Nov. 5, 1975. pp. 46–52.

B. Commissions

U.S. Commission on CIA Activities Within the United States. Report, Washington, D.C.: U.S. Govt. Print. Off., June 6, 1975; 3–9.
U.S. Commission on the Organization of the Government for the Conduct of Foreign Policy. Intelligence support for foreign policy in the future (prepared by Russell Jack Smith). Vol. 7, Appendix U. Washington, D.C.: U.S. Govt. Print. Off., 1975: 84–86.
U.S. Commission on the Organization of the Government for the Conduct of Foreign Policy. Problems in the conduct of United States foreign policy: a compilation of recent criticism (prepared by J. Daniel O'Flaherty). Vol. 7, Appendix X. Washington, D.C.: U.S. Govt. Print. Off., 1975: 335
U.S. Department of Justice. Federal Committee on False Identification. Proposed findings and recommendations. Federal Register. V. 41, no 117. June 16, 1976: 24431–24437.
U.S. National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. Electronic surveillance. Washington, D.C.: U.S. Govt. Print. Off., 1976: xi-xix.
U.S. Privacy Protection Study Commission. Federal tax return confidentiality. Washington, D.C.: U.S. Govt. Print. Off., 1976: 1–8.

C. Courts

Director of the Administrative Office of the United States Courts. Report of the Director on applications for orders authorizing or approving the interception of wire or oral communications for the period Jan. 1, 1975 to Dec. 31, 1975. (Washington, D.C.) April 30, 1976. pp. i-v.
U.S. National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. State of the law of electronic surveillance (Commission studies). Washington, D.C.: U.S. Govt. Print. Off., 1976. pp. 1–24.

[From the Federal Register, Vol. 40, May 20, 1975]

A. Executive Branch

TITLE 28—JUDICIAL ADMINISTRATION

CHAPTER I—DEPARTMENT OF JUSTICE

[Order No. 601–75]

PART 20—CRIMINAL JUSTICE INFORMATION SYSTEMS

This order establishes "regulations governing the dissemination of criminal record and criminal history information and includes a commentary on selective sections as an appendix. Its purpose is to afford greater protection of the privacy of individuals who may be included in the records of the Federal Bureau of Investigation, criminal justice agencies receiving funds directly or indirectly from the Law Enforcement Assistance Administration, and interstate, state or local criminal justice agencies exchanging records with the FBI or these federally-funded systems." At the same time, these regulations preserve legitimate law enforcement need for access to such records.

Pursuant to the authority vested in the Attorney General by 28 U.S.C. 509, 510, 534, and Pub. L. 92–544, 86 Stat. 1115, and 5 U.S.C. 301 and the authority vested in the Law Enforcement Assistance Administration by sections 501 and 524 of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973, Pub L. 93–83, 87 Stat. 197 (42 U.S.C. § 3701 et seq. (Aug. 6, 1973)), this addition to Chapter I of Title 28 of the Code of Federal Regulations is issued as Part 20 by the Department of Justice to become effective June 19, 1975.

This addition is based on a notice of proposed rule making published in the Federal Register on February 14, 1974 (39 FR 5636). Hearings on the proposed regulations were held in Washington, D.C. in March and April and in San Francisco, California in May 1974. Approximately one hundred agencies, organizations and individuals submitted their suggestions and comments, either orally or in writing. Numerous changes have been made in the regulations as a result of the comments received.

Subpart A—General Provisions

Sec.

20.1 Purpose.
20.2 Authority.
20.3 Definitions.

Subpart B—State and Local Criminal History Record Information Systems

20.20 Applicability.
20.21 Preparation and submission of a Criminal History Record Information Plan.
20.22 Certification of Compliance.
20.23 Documentation: Approval by LEAA.
20.24 State laws on privacy and security.
20.25 Penalties.
20.26 References.

Subpart C—Federal System and Interstate Exchange of Criminal History Record Information

20.30 Applicability.
20.31 Responsibilities.
20.32 Includable offenses.
20.33 Dissemination of criminal history record information.
20.34 Individual's right to access criminal history record information.
20.35 National Crime Information Center Advisory Policy Board.
20.36 Participation in the Computerized Criminal History Program.
20.37 Responsibility for accuracy, completeness, currency.
20.38 Sanction for noncompliance.

Authority: Pub. L. 93–83, 87 Stat. 197, (42 U.S.C. 3701, et seq.; 28 U.S.C. 534), Pub. L. 92–544, 86 Stat. 1115.

Subpart A—General Provisions

§ 20.1 Purpose.

It is the purpose of these regulations to assure that criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the completeness; integrity, accuracy and security of such information and to protect individual privacy.

§ 20.2 Authority.

These regulations are issued pursuant to section 501 and 524(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973, Pub. L. 93–83, 87 Stat. 197, 42 U.S.C. 3701, et seq. (Act), 28 U.S.C. 534, and Pub. L. 92–544, 86 Stat. 1115.

§ 20.3 Definitions.

As used in these regulations:

(a) "Criminal history record information system" means a system including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation or dissemination of criminal history record information.

(b) "Criminal history record information" means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system.

(c) "Criminal justice agency" means: (1) courts; (2) a government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.

(d) The "administration of criminal justice" means performance of any of the following activities; detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

(e) "Disposition" means information disclosing that criminal proceedings have been concluded, including information disclosing that

the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings and also disclosing the nature of the termination in the proceedings; or information disclosing that proceedings have been indefinitely postponed and also disclosing the reason for such postponement. Dispositions shall include, but not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed—civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial—defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.

(f) "Statute" means an Act of Congress or State legislature of a provision of the Constitution of the United States or of a State.

(g) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(h) An "executive order" means an order of the President of the United States or the Chief Executive of a State which has the force of law and which is published in a manner permitting regular public access thereto.

(i) "Act" means the Omnibus Crime Control and Safe Streets Act, 42 U.S.C. 3701 et seq. as amended.

(j) "Department of Justice criminal history record information system" means the Identification Division and the Computerized Criminal History File systems operated by the Federal Bureau of Investigation.

Subpart B—State and Local Criminal History Record information Systems

§ 20.20 Applicability.

(a) The regulations in this subpart apply to all State and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations where such collection, storage, or dissemination has been funded in whole or in part with funds made available by the Law Enforcement Assistance Administration subsequent to July 1, 1973, pursuant to Title I of the Act.

(b) The regulations in this subpart shall not apply to criminal history record information contained in: (1) porters, announcements, or lists for identifying or apprehending fugitives or wanted persons; (2) original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis; (3) court records of public judicial proceedings compiled chronologically; (4) published court opinions or public judicial proceedings; (5) records of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof

for the purpose of regulating the issuance suspension revocation or renewal of driver's, pilot's or other operators' licenses; (6) announcements of executive clemency.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates. Nor is a criminal justice agency prohibited from confirming prior criminal history record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, on a specified date, if the arrest record information or criminal record information disclosed is based on data excluded by paragraph (b) of this section.

§ 20.21 Preparation and submission of a Criminal History Record Information Plan.

A plan shall be submitted to LEAA by each State within 180 days of the promulgation of these regulations. The plan shall set forth operational procedures to—

(a) *Completeness and accuracy.*—Insure that criminal history record information is complete and accurate.

(1) Complete records should be maintained at a central State repository. To be complete, a record maintained at a central State repository which contains information that an individual has been arrested, and which is available for dissemination, must contain information of any dispositions occurring within the State within 90 days after the disposition has occurred. The above shall apply to all arrests occurring subsequent to the effective date of these regulations. Procedures shall be established for criminal justice agencies to query the central repository prior to dissemination of any criminal history record information to assure that the most up-to-date disposition data is being used. Inquires of a central State repository shall be made prior to any dissemination except in those cases where time is of the essence and the repository is technically incapable of responding within the necessary time period. (2) To be accurate means that no record containing criminal history record information shall contain erroneous information. To accomplish this end, criminal justice agencies shall institute a process of data collection, entry, storage, and systematic audit that will minimize the possibility of recording and storing inaccurate information and upon finding inaccurate information of a material nature, shall notify all criminal justice agencies known to have received such information.

(b) *Limitations on dissemination.*—Insure that dissemination of criminal history record information has been limited, whether directly or through any intermediary only to:

(1) Criminal justice agencies, for purposes of the administration of criminal justice and criminal justice agency employment;

(2) Such other individuals and agencies which require criminal history record information to implement a statute or executive order that expressly refers to criminal conduct and contains requirements and/or exclusions expressly based upon such conduct;

(3) Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice pursuant to that agreement. The agreement shall specifically authorize access to data, limit the use of data to purposes for which given, insure the security and confidentiality of the data consistent with these regulations, and provide sanctions for violation thereof;

(4) Individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency. The agreement shall specifically authorize access to data, limit the use of data to research, evaluative, or statistical purposes, insure the confidentiality and security of the data consistent with these regulations and with section 524(a) of the Act and any regulations implementing section 524(a), and provide sanctions for the violation thereof;

(5) Agencies of State or federal government which are authorized by statute or executive order to conduct investigations determining employment suitability or eligibility for security clearances allowing access to classified information; and

(6) Individuals and agencies where authorized by court order or court rule.

(c) *General policies on use and dissemination.*—Insure adherence to the following restrictions:

(1) Criminal history record information concerning the arrest of an individual may not be disseminated to a non-criminal justice agency or individual (except under § 20.21(b) (3), (4), (5), (6)) if an interval of one year has elapsed from the date of the arrest and no disposition of the charge has been recorded and no active prosecution of the charge is pending;

(2) Use of criminal history record information disseminated to non-criminal justice agencies under these regulations shall be limited to the purposes for which it was given and may not be disseminated further.

(3) No agency or individual shall confirm the existence or non-existence of criminal history record information for employment or licensing checks except as provided in paragraphs (b) (1), (b) (2), and (b) (5) of this section.

(4) This paragraph sets outer limits of dissemination. It does not, however, mandate dissemination of criminal history record information to any agency or individual.

(d) *Juvenile records.*—Insure that dissemination of records concerning proceedings relating to the adjudication of a juvenile as delinquent or in need or supervision (or the equivalent) to noncriminal justice agencies is prohibited, unless a statute or Federal executive order specifically authorizes dissemination of juvenile records, except to the same extent as criminal history records may be disseminated as provided in § 20.21 (b) (3), (4), and (6).

(e) *Audit.*—Insure that annual audits of a representative sample of State and local criminal justice agencies chosen on a random basis shall be conducted by the State to verify adherence to these regulations and that appropriate records shall be retained to facilitate such audits. Such records shall include, but are not limited to, the names of

all persons or agencies to whom information is disseminated and the date upon which such information is disseminated.

(f) *Security.*—Insure confidentiality and security of criminal history record information by providing that wherever criminal history record information is collected, stored, or disseminated a criminal justice agency shall—

(1) Institute where computerized data processing is employed effective and technologically advanced software and hardware designs to prevent unauthorized access to such information;

(2) Assure that where computerzied data processing is employed, the hardware, including processor, communications control, and storage device, to be utilized for the handling of criminal history record information is dedicated to purposes related to the administration of criminal justice;

(3) Have authority to set and enforce policy concerning computer operations;

(4) Have power to veto for legitimate security purposes which personnel can be permitted to work in a defined area where such information is stored, collected, or disseminated.

(5) Select and supervise all personnel authorized to have direct access to such information;

(6) Assure that an individual or agency authorized direct access is administratively held responsible for (i) the physical security of criminal history record information under its control or in its custody and (ii) the protection of such information from unauthorized accesses, disclosure, or dissemination;

(7) Institute procedures to reasonably protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or man-made disasters;

(8) Provide that each employee working with or having access to criminal history record information should be made familiar with the substance and intent of these regulations; and

(9) Provide that direct access to criminal history records information shall be available only to authorized officers or employees of a criminal justice agency.

(g) *Access and review.* Insure the individual's right to access and review of criminal history information for purposes of accuracy and completeness by instituting procedures so that—

(1) Any individual shall, upon satisfactory verification of his identity be entitled to review without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction;

(2) Administative review and necessary correction of any claim by the individual to whom the information relates that the information is inaccurate or incomplete is provided;

(3) The State shall establish and implement procedures for administrative appeal where a criminal justice agency refuses to correct challenged information to the satisfaction of the individual to whom the information relates;

(4) Upon request, an individual whose record has been corrected shall be given the names of all non-criminal justice agencies to whom the data has been given;

(5) The correcting agency shall notify all criminal justice recipients of corrected information; and

(6) The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigatory, or other related files and shall not be construed to include any other information than that defined by § 20.3(b).

§ 20.22 Certification of Compliance.

(a) Each State to which these regulations are applicable shall with the submission of each plan provide a certification that to the maximum extent feasible action has been taken to comply with the procedures set forth in the plan. Maximum extent feasible, in this subsection, means actions which can be taken to comply with the procedures set forth in the plan that do not require additional legislative authority or involve unreasonable cost or do not exceed existing technical ability.

(b) The certification shall include—

(1) An outline of the action which has been instituted. At a minimum, the requirements of access and review under 20.21(g) must be completely operational;

(2) A description of any legislation or executive order, or attempts to obtain such authority that has been instituted to comply with these regulations;

(3) A description of the steps taken to overcome any fiscal, technical, and administrative barriers to the development of complete and accurate criminal history record information;

(4) A description of existing system capability and steps being taken to upgrade such capability to meet the requirements of these regulations; and

(5) A listing setting forth all noncriminal justice dissemination authorized by legislation existing as of the date of the certification showing the specific categories of non-criminal justice individuals or agencies, the specific purposes or uses for which information may be disseminated, and the statutory or executive order citations.

§ 20.23 Documentation: Approval by LEAA.

Within 90 days of the receipt of the plan, LEAA shall approve or disapprove the adequacy of the provisions of the plan and certification. Evaluation of the plan by LEAA will be based upon whether the procedures set forth will accomplish the required objectives. The evaluation of the certification(s) will be based upon whether a good faith effort has been shown to initiate and/or further compliance with the plan and regulations. All procedures in the approved plan must be fully operational and implemented by December 31, 1977, except that a State, upon written application and good cause, may be allowed an additional period of time to implement § 20.21(f)(2). Certification shall be submitted in December of each year to LEAA until such complete compliance. The yearly certification shall update the information provided under § 20.21.

79-064 O - 76 - 25

§ 20.24 State laws on privacy and security.

Where a State originating criminal history record information provides for sealing or purging thereof, nothing in these regulations shall be construed to prevent any other State receiving such information, upon notification, from complying with the originating State's sealing or purging requirements.

§ 20.25 Penalties.

Any agency or individual violating subpart B of these regulations shall be subject to a fine not to exceed $10,000. In addition, LEAA may initiate fund cut-off procedures against recipients of LEAA assistance.

Subpart C—Federal System and Interstate Exchange of Criminal History Record Information

§ 20.30 Applicability.

The provisions of this subpart of the regulations apply to any Department of Justice criminal history record information system that serves criminal justice agencies in two or more states and to Federal, state and local criminal justice agencies to the extent that they utilize the services of Department of Justice criminal history record information systems. These regulations are applicable to both manual and automated systems.

§ 20.31 Responsibilities.

(a) The Federal Bureau of Investigation (FBI) shall operate the National Crime Information Center (NCIC), the computerized information system which includes telecommunications lines and any message switching facilities which are authorized by law or regulation to link local, state and Federal criminal justice agencies for the purpose of exchanging NCIC-related information. Such information includes information in the Computerized Criminal History (CCH) File, a cooperative Federal-State program for the interstate exchange of criminal history record information. CCH shall provide a central repository and index of criminal history record information for the purpose of facilitating the interstate exchange of such information among criminal justice agencies.

(b) The FBI shall operate the Identification Division to perform identification and criminal history record information functions for Federal, state and local criminal justice agencies, and for noncriminal justice agencies and other entities where authorized by Federal statute, state statute pursuant to Public Law 92–544 (86 Stat. 1115), Presidential executive order, or regulation of the Attorney General of the United States.

(c) The FBI Identification Division shall maintain the master fingerprint files on all offenders included in the NCIC/CCH File for the purposes of determining first offender status and to identify those offenders who are unknown in states where they become criminally active but known in other states through prior criminal history records.

§ 20.32 Includable offenses.

(a) Criminal history record information maintained in any Department of Justice criminal history record information system shall include serious and/or significant offenses.

(b) Excluded from such a system are arrests and court actions limited only to nonserious charges, e.g., drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, nonspecific charges of suspicion or investigation, traffic violations (except data will be included on arrests for manslaughter, driving under the influence of drugs or liquor, and hit and run). Offenses committed by juvenile offenders shall also be excluded unless a juvenile offender is tried in court as an adult.

(c) The exclusions enumerated above shall not apply to Federal manual criminal history record information collected, maintained and compiled by the FBI prior to the effective date of these Regulations.

§ 20.33 Dissemination of criminal history record information.

(a) Criminal history record information contained in any Department of Justice criminal history record information system will be made available:

(1) To criminal justice agencies for criminal justice purposes; and

(2) To Federal agencies authorized to receive it pursuant to Federal statute or Executive order.

(3) Pursuant to Public Law 92–544 (86 Stat. 115) for use in connection with licensing or local/state employment or for other uses only if such dissemination is authorized by Federal or state statutes and approved by the Attorney General of the United States. When no active prosecution of the charge is known to be pending arrest data more than one year old will not be disseminated pursuant to this subsection unless accompanied by information relating to the disposition of that arrest.

(4) For issuance of press releases and publicity designed to effect the apprehension of wanted persons in connection with serious or significant offenses.

(b) The exchange of criminal history record information authorized by paragraph (a) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates.

§ 20.34 Individual's right to access criminal history record information.

(a) Any individual, upon request, upon satisfactory verification of his identity by fingerprint comparison and upon payment of any required processing fee, may review criminal history record informa-

tion maintain about him in a Department of Justice criminal history record information system.

(b) If, after reviewing his identification record, the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections or updating of the alleged deficiency, he must make application directly to the contributor of the questioned information. If the contributor corrects the record, it shall promptly notify the FBI and, upon receipt of such a notification, the FBI will make any changes necessary in accordance with the correction supplied by the contributor of the original information.

§ 20.35 National Crime Information Center Advisory Policy Board

There is established in NCIC Advisory Policy Board whose purpose is recommend to the Director, FBI, general policies with respect to the philosophy, concept and operational principles of NCIC, particularly its relationships with local and state systems relating to the collection, processing, storage, dissemination and use of criminal history record information contained in the CCH File.

(a) (1) The Board shall be composed of twenty-six members, twenty of whom are elected by the NCIC users from across the entire United States and six who are appointed by the Director of the FBI. The six appointed members, two each from the judicial, the corrections and the prosecutive sectors of the criminal justice community, shall serve for an indeterminate period of time. The twenty elected members shall serve for a term of two years commencing on January 5th of each odd numbered year.

(2) The Board shall be representative of the entire criminal justice community at the state and local levels and shall include representation from law enforcement, the courts and corrections segments of this community.

(b) The Board shall review and consider rules, regulations and procedures for the operation of the NCIC.

(c) The Board shall consider operational needs of criminal justice agencies in light of public policies, and local, state and Federal statues and these Regulations.

(d) The Board shall review and consider security and privacy aspects of the NCIC system and shall have a standing Security and Confidentiality Committee to provide input and recommendations to the Board concerning security and privacy of the NCIC system on a continuing basis.

(e) The Board shall recommend standards for participation by criminal justice agencies in the NCIC system.

(f) The Board shall report directly to the Director of the FBI or his designated appointee.

(g) The Board shall operate within the purview of the Federal Advisory Committee Act. Public Law 92–463, 86 Stat. 770.

(h) The Director, FBI, shall not adopt recommendations of the Board which would be in violation of these Regulations.

§ 20.36 Participation in the Computerized Criminal History Program

(a) For the purpose of acquiring and retaining direct access to CCH File each criminal justice agency shall execute a signed agreement with the Director, FBI, to abide by all present rules, policies

and procedures of the NCIC, as well as any rules, policies and procedures hereinafter approved by the NCIC Advisory Policy Board and adopted by the NCIC.

(b) Entry of criminal history record information into the CCH File will be accepted only from an authorized state or Federal criinal justice control terminal. Terminal devices in other authorized criminal justice agencies will be limited to inquiries.

§ 20.37 Responsibility for accuracy, completeness, currency

It shall be the responsibility of each criminal justice agency contriuting data to any Department of Justice criminal history record information system to assure that information on individuals is kept complete, accurate and current so that all such records shall contain to the maximum extent feasible dispositions for all arrest data included therein. Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred.

§ 20.38 Sanction for noncompliance

The services of Department of Justice criminal history record information systems are subject to cancellation in regard to any agency or entity which fails to comply with the provisions of Subpart C.

EDWARD H. LEVI,
Attorney General.
RICHARD W. VELDE,
Administrator, Law Enforcement Assistance Administration.
MAY 15, 1976.

APPENDIX—COMMENTARY ON SELECTED SECTIONS OF THE REGULATIONS ON CRIMINAL HISTORY RECORD INFORMATION SYSTEMS

Subpart A—§ *20.3(b)*. The definition of criminal history record information is intended to include the basic offender-based transaction statistics/computerized criminal history (OBTS/CCH) data elements. If notations of an arrest, disposition, or other formal criminal justice transactions occur in records other than the traditional "rap sheet" such as arrest reports, any criminal history record information contained in such reports comes under the definition of this subsection.

The definition, however, does not extend to other information contained in criminal justic agency reports. Intelligence or investigative information (e.g. suspected criminal activity, associates, hangouts, financial information, ownership of property and vehicles) is not included in the definition of criminal history information.

§ *20.3(c)*. The definition of criminal justice agency and administration of criminal justice of 20.3(c)(d) must be considered together. Included as criminal justice agencies would be traditional police, courts, and corrections agencies as well as subunits of noncriminal justice agencies performing a function of the administration of criminal justice pursuant to Federal or State statute or executive order. The above subunits of non-criminal justice agencies would include for example, the Office of Investigation of the U.S. Department of Agriculture which has as its principal function the collection of evidence for criminal prosecutions of fraud. Also included under the definition

of criminal justice agency are umbrella-type administrative agencies supplying criminal history information services such as New York's Division of Criminal Justice Services.

§ 20.3(e). Disposition is a key concept in the section 524(b) of the Act and in § 2021(a)(1) and § 20.21(b)(2). It, therefore, is defined in this subsection are examples only and are not to be construed as excluding other unspecified transactions concluding criminal proceedings within a particular agency.

Subpart B—§ 20.20(a). These regulations apply to criminal justice agencies receiving Safe Streets funds for manual or automated systems subsequent to July 1, 1973. In the hearings on the regulations, a number of those testifying challenged LEAA's authority to promulgate regulations for manual systems by contending that section 524(b) of the Act governs criminal history information contained in automated systems.

The intent of section 524(b), however, would be subverted by only regulating automated systems. Any agency that wished to circumvent the regulations would be able to create duplicate manual files for purposes contrary to the letter and spirit of the regulations.

Regulations of manual systems, therefore, is authorized by section 524(b) when coupled with Section 501 of the Act which authorizes the Administration to establish rules and regulations "necessary to the exercise of its functions * * *."

The Act clearly applies to all criminal history record information collected, stored, or disseminated with LEAA support subsequent to July 1, 1973.

§ 20.20(b)(c). Section 20.20(b)(c) exempts from regulations certain types of records vital to the apprehension of fugitives, freedom of the press, and the public's right to know.

Section 20.20(b)(ii) attempts to deal with the problem of computerized police blotters. In some local jurisdictions, it is apparently possible for private individuals and/or newsmen upon submission of a specific name to obtain through a computer search of the blotter a history of a person's arrests. Such files create a partial criminal history data bank potentially damaging to individual privacy, especially since they do not contain final dispositions. By requiring that such records be accessed solely on a chronological basis, the regulations limit inquiries to specific time periods and discourage general fishing expeditions into a person's private life.

Subsection 20.20(c) recognizes that announcements of ongoing developments in the criminal justice process should not be precluded from public disclosure. Thus announcements of arrest, convictions, new developments in the course of an investigation may be made within a few days of their occurrence. It is also permissible for a criminal justice agency to confirm certain matters of public record information upon specific inquiry. Thus, if a question is raised: "Was X arrested by your agency on January 3, 1952" and this can be confirmed or denied by looking at one of the records enumerated in subsection (b) above, then the criminal agency may respond to the inquiry.

§ 20.21. Since privacy and security considerations are too complex to be dealt with overnight, the regulations require a State plan to

assure orderly progress toward the objectives of the Act. In response to requests of those testifying on the draft regulations, the deadline for submission of the plan was set at 180 days. The kind of planning document anticipated would be much more concise than, for example, the State's criminal justice comprehensive plan.

The regulations deliberately refrain from specifying who within a State should be responsible for preparing the plan. This specific determination should be made by the Governor.

§ *20.21(a)(1)*. Section 524(b) of the Act requires that LEAA insure criminal history information be current and that, to the maximum extent feasible, it contain disposition as well as current data.

It is, however, economically and administratively impractical to maintain complete criminal histories at the local level. Arrangements for local police departments to keep track of dispositions by agencies outside of the local jurisdictions generally do not exist. It would, moreover, be bad public policy to encourage such arrangements since it would result in an expensive duplication of files.

The alternatives to locally kept criminal histories are records maintained by a central State repository. A central State repository is a State agency having the function pursuant to statute or executive order of maintaining comprehensive statewide criminal history record information files. Ultimately through automatic data processing the State level will have the capability to handle all requests for in-State criminal history information.

Section 20.21(a)(1) is written with a centralized State criminal history repository in mind. The first sentence of the subsection states that complete records should be retained at a central State repository. The word "should" is permissive; it suggests but does not mandate a central State repoitory.

The regulations do require that States establish procedures for State and local criminal justice agencies to query central State repositories wherever they exist. Such procedures are intended to insure that the most current criminal justice information is used.

As a minimum, criminal justice agencies subject to these regulations must make inquiries of central State repositories whenever the repository is capable of meeting the user's request within a reasonable time. Presently, comprehensive records of an individual's transactions within a State are maintained in manual files at the State level, if at all. It is probably unrealistic to expect manual systems to be able immediately to meet many rapid-acess needs of police and prosecutors. On the other hand, queries of the State central repository for most noncriminal justice purposes probably can and should be made prior to dissemination of criminal history record information.

§ *20.21(b)*. The limitations on dissemination in this subsection are essential to fulfill the mandate of section 524(b) of the Act which requires the Administration to assure that the "privacy of all information is adequately provided for and that information shall only be used for law enforcement and criminal justice and other lawful purposes." The categories for dissemination established in this section reflect suggestions by hearing witnesses and respondents submitting written commentary.

§ *20.21(b)(2)*. This subsection is intended to permit public or private agencies to have access to criminal history record information where a statute or executive order:

(1) Denies employment, licensing, or other civil rights and privileges to persons convicted of a crime;

(2) Requires a criminal record check prior to employment, licensing, etc.

The above examples represent statutory patterns contemplated in drafting the regulations. The sine qua non for dissemination under this subsection is statutory reference to criminal conduct. Statutes which contain requirements and/or exclusions based on "good moral character" or "trust worthiness" would not be sufficient to authorize dissemination.

The language of the subsection will accommodate Civil Service suitability investigations under Executive Order 10450, which is the authority for most investigations conducted by the Commission. Section 3(a) of 10450 prescribes the minimum scope of investigation and requires a check of FBI fingerprint files and written inquires to appropriate law enforcement agencies.

§ *20.21(b)(3)*. This subsection would permit private agencies such as the Vera Institute to receive criminal histories where they perform a necessary administration of justice function such as pretrial release. Private consulting firms which commonly assist criminal justice agencies in information systems development would also be included here.

§ *20.21(b)(4)*. Under the subsection, any good faith researchers including private individuals would be permitted to use criminal history record information for research purposes. As with the agencies designated in § 20.21(b)(3) researchers would be bound by an agreement with the disseminating criminal justice agency and would, of course, be subject to the sanctions of the Act.

The drafters of the regulations expressly rejected a suggestion which would have limited access for research purposes to certified research organizations. Specially "certification" criteria would have been extremely difficult to draft and would have inevitably led to unnecessary restrictions on legitimate research.

Section 524(a) of the Act which forms part of the requirements of this section states:

> Except as provided by Federal law other than this title, no officer or employee of the Federal Government, nor any recipient of assistance under the provisions of this title shall use or reveal any research or statistical information furnished under this title by any person and identifiable to any specific private person for any purpose other than the purpose for which it was obtained in accordance with this title. Copies of such information shall be immune from legal process, and shall not, without the consent of the person furnishing such information, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceedings.

LEAA anticipates issuing regulations pursuant to Section 524(a) as soon as possible.

§ *20.21(b)(5)*. Dissemination under this section would be permitted not only in cases of investigations of employment suitability, but also investigations relating to clearance of individuals for access to information which is classified pursuant to Executive Order 11652.

§ *20.21(c)(1)*. "Active prosecution pending" would mean, for example, that the case is still actively in process, the first step such as an arraignment has been taken and the case docketed for court trial. This term is not intended to include any treatment alternative-type program which might defer prosecution to a later date. Such a deferral prosecution is a disposition which should be entered on the record.

§ *20.21(c)(3)*. Presently some employers are circumventing State and local dissemination restrictions by requesting applicants to obtain an official certification of no criminal record. An employer's request under the above circumstances gives the applicant the unenviable choice of his privacy or loss of possible job opportunities. Under this subsection routine certifications of no record would no longer be permitted. In extraordinary circumstances, however, an individual could obtain a court order permitting such a certification.

§ *20.21(c)(4)*. The language of this subsection leaves to the States the question of who among the agencies and individuals listed in § 20.21(b) shall actually receive criminal records. Under these regulations a State could place a total ban on dissemination if it so wished.

§ *20.21(d)*. Non-criminal justice agencies will not be able to receive records of juveniles unless the language or statute or Federal executive order specifies that juvenile records shall be available for dissemination. Perhaps the most controversial part of this subsection is that it denies access to records of juveniles by Federal agencies conducting background investigations or eligibility to classified information under existing legal authority.

§ *20.21(e)*. Since it would be too costly to audit each criminal justice agency in most States (Wisconsin, for example, has 1075 criminal justice agencies) random audits of a "representative sample" of agencies are the next best alternative. The term "representative sample" is used to insure that audits do not simply focus on certain types of agencies.

§ *20.21(f)(2)*. In the short run, dedication will probably mean greater costs for State and local governments. How great such costs might be is dependent upon the rapidly advancing state of computer technology. So that there will be no serious hardship on States and localities as a result of this requirement, § 20.23 provides that additional time will be allowed to implement the dedication requirement. For example, where local systems now in place contain criminal history information of only that State, used purely for intrastate purposes, in a shared environment, consideration will be given to granting extensions of time under this provision.

§ *20.21(f)(5), (8)*. "Direct access" means that any non-criminal agency authorized to receive criminal justice data must go through a criminal justice agency to obtain information.

§ *20.21(g)(1)*. A "challenge" under this section is an oral or written contention by an individual that his record is inaccurate or incomplete; it would require him to give a correct version of his record and explain why he believes his version to be correct. While an individual should have access to his record for review, a copy of the record should ordinarily only be given when it is clearly established that it is necessary for the purpose of challenge.

The drafters of the subsection expressly rejected a suggestion that would have called for a satisfactory verification of identity by fingerprint comparison. It was felt that states ought to be free to determine other means of identity verification.

§ *20.21(g)(5)*. Not every agency will have done this in the past, but henceforth adequate records including those required under § 20.21 (e) must be kept so that notification can be made.

§ *20.21(g)(6)*. This section emphasizes that the right to access and review extends only to criminal history information and does not include other information such as intelligence or treatment data.

§ *20.22(a)*. The purpose for the certification requirement is to initiate immediate compliance with these regulations wherever possible. The term "maximum extent feasible" acknowledges that there are some areas such as the completeness requirement which create complex legislative and financial problems.

NOTE: In preparing the plans required by these regulations, States should look for guidance to the following documents: National Advisory Commission on Criminal Justice Standards and Goals, Report on the Criminal Justice System; Project SEARCH: Security and Privacy Considerations in Criminal History Information Systems, Technical Report #2; Project SEARCH: A Model State Act for Criminal Offender Record Information, Technical Memorandum #3; and Project SEARCH: Model Administrative Regulations for Criminal Offender Record Information, Technical Memorandum #4.

Subpart C—§ *20.31*. Defines the criminal history record information system operated by the Federal Bureau of Investigation. Each state having a record in the Computerized Criminal History (CCH) file must have a fingerprint card on file in the FBI Identification Division to support the CCH record concerning the individual.

Paragraph b is not intended to limit the identification services presently performed by the FBI for Federal, state and local agencies.

§ *20.32*. The grandfather clause contained in the third paragraph of this Section is designed, from a practical standpoint, to eliminate the necessity of deleting from the FBI's massive files the non-includable offenses which were stored prior to February, 1973.

In the event a person is charged in court with a serious or significant offense arising out of an arrest involving a non-includable offense, the non-includable offense will appear in the arrest segment of the CCH record.

§ *20.33*. Incorporates the provisions of a regulation issued by the FBI on June 26, 1974, limiting dissemination of arrest information not accompanied by disposition information outside the Federal government for non-criminal justice purposes. This regulation is cited in 28 CFR 50.12.

§ *20.34*. The procedures by which an individual may obtain a copy of his manual identification record are particularized in 28 CFR 16.30–34.

The procedures by which an individual may obtain a copy of his Computerized Criminal History are as follows:

If an individual has a criminal record supported by fingerprints and that record has been entered in the NCIC CCH File, it is available to that individual for review, upon presentation of appropriate

identification, and in accordance with applicable state and Federal administrative and statutory regulations.

Appropriate identification includes being fingerprinted for the purpose of insuring that he is the individual that he purports to be. The record on file will then be verified as his through comparison of fingerprints.

Procedure. 1. All requests for review must be made by the subject of his record through a law enforcement agency which has access to the NCIC CCH File. That agency within statutory or regulatory limits can require additional identification to assist in securing a positive identification.

2. If the cooperating law enforcement agency can make an identification with fingerprints previously taken which are on file locally and if the FBI identification number of the individual's record is available to that agency, it can make an on-line inquiry of NCIC to obtain his record on-line or, if it does not have suitable equipment to obtain an on-line response, obtain the record from Washington, D.C., by mail. The individual will then be afforded the opportunity to see that record.

3. Should the coopearting law enforcement agency not have the individual's fingerprints on file locally, it is necessary for that agency to relate his prints to an existing record by having his identification prints compared with those already on file in the FBI or, possibly, in the State's central identification agency.

4. The subject of the requested record shall request the appropriate arresting agency, court, or correctional agency to initiate action necessary to correct any stated inaccuracy in his record or provide the information needed to make the record complete.

§ *20.36.* This section refers to the requirements for obtaining direct access to the CCH file. One of the requirements is that hardware, including processor, communications control and storage devices, to be utilized for the handling of criminal history data must be dedicated to the criminal justice function.

§ *20.37.* The 120-day requirement in his section allows 30 days more than the similar provision in Subpart B in order to allow for processing time which may be needed by the state before forwarding the disposition to the FBI.

[FR Doc.75-13197 Filed 5-19-75;8:45 am]

[Order No. 602-75]

Part 50—Statements of Policy

Release of Information by Personnel of the Department of Justice Relating to Criminal and Civil Proceedings

This order amends the Department of Justice guidelines concerning the release of information by personnel of the Department of Justice relating to criminal and civil proceedings by deleting the provision permitting disclosure of criminal history record information on request.

By virtue of the authority vested in me as Attorney General of the United States, § 50.2(b) (4) of Chapter I, Title 28 of the Code of Federal Regulations is amended to read as follows:

§ 50.2 Release of information by personnel of the Department of Justice relating to criminal and civil proceedings.

* * * * * * *

(b) * * *

* * * * * * *

(4) Personnel of the Department shall not disseminate any information concerning a defendant's prior criminal record.

* * * * * * *

MAY 15, 1975.

EDWARD H. LEVI,
Attorney General.

[FR Doc.75-13198 Filed 5-19-75;8:45 am]

U.S. Department of Justice. Guidelines for domestic security investigations, White House personnel security and background investigations, and reporting on civil disorders and demonstrations involving a Federal interest. March 10, 1976 (Washington, D.C.) 20 p.

DOMESTIC SECURITY INVESTIGATIONS

I. BASES OF INVESTIGATION

A. Domestic security investigations are conducted, when authorized under Section II(C), II(F), or II(I), to ascertain information on the activities of individuals, or the activities of groups, which involve or will involve the use of force or violence and which involve or will involve the violation of federal law, for the purpose of:

(1) overthrowing the government of the United States or the government of a State;

(2) substantially interfering, in the United States, with the activities of a foreign government or its authorized representatives;

(3) substantially impairing for the purpose of influencing U.S. government policies or decisions:

(a) the functioning of the government of the United States;

(b) the functioning of the government of a State; or

(c) interstate commerce.

(4) depriving persons of their civil rights under the Constitution, laws, or treaties of the United States.

II. INITIATION AND SCOPE OF INVESTIGATIONS

A. Domestic security investigations are conducted at three levels -- preliminary investigations, limited investigations, and full investigations -- differing in scope and in investigative techniques which may be used.

B. All investigations undertaken through these guidelines shall be designed and conducted so as not to limit the full exercise of rights protected by the Constitution and laws of the United States.

Preliminary Investigations

C. Preliminary investigations may be undertaken on the basis of allegations or other information that an individual or a group may be engaged in activities which involve or will involve the use of force or violence and which involve or will involve the

violation of federal law for one or more of the purposes enumerated in IA(1)-IA(4). These investigations shall be confined to determining whether there is a factual basis for opening a full investigation.

D. Information gathered by the FBI during preliminary investigations shall be pertinent to verifying or refuting the allegations or information concerning activities described in paragraph IA.

E. FBI field offices may, on their own initiative, undertake preliminary investigations limited to:

1. examination of FBI indices and files;

2. examination of public records and other public sources of information;

3. examination of federal, state, and local records;

4. inquiry of existing sources of information and use of previously established informants; and

5. physical surveillance and interviews or persons not mentioned in E(1)-E(4) for the limited purpose of identifying the subject of an investigation.

Limited Investigations

F. A limited investigation must be authorized in writing by a Special Agent in Charge or FBI Headquarters when the techniques listed in paragraph E are inadequate to determine if there is a factual basis for a full investigation. In addition to the techniques set forth in E(1)-E(4) the following techniques also may be used in a limited investigation:

1. physical surveillance for purposes other than identifying the subject of the investigation;

2. interviews of persons not mentioned in E(1)-E(4) for purposes other than identifying the subject of the investigation, but only when authorized by the Special Agent in Charge after full consideration of such factors as the seriousness of the allegation, the need for the interview, and the consequences of using the technique. When there is a question whether an interview should be undertaken, the Special Agent in Charge shall seek approval of FBI Headquarters.

G. Techniques such as recruitment or placement of informants in groups, "mail covers," or electronic surveillance, may not be used as part of a preliminary or a limited investigation.

H. All preliminary and limited investigations shall be closed within 90 days of the date upon which the preliminary investigation was initiated. However, FBI Headquarters may authorize in writing extension of a preliminary or limited investigation for periods of not more than 90 days when facts or information obtained in the original period justify such an extension. The authorization shall include a statement of the circumstances justifying the extension.

Full Investigation

I. Full investigations must be authorized by FBI Headquarters. They may only be authorized on the basis of specific and articulable facts giving reason to believe that an individual or a group is or may be engaged in activities which involve the use of force or violence and which involve or will involve the violation of federal law for one or more of the purposes enumerated in IA(1)-IA(4). The following factors must be considered in determining whether a full investigation should be undertaken:

(1) the magnitude of the threatened harm;

(2) the likelihood it will occur;

(3) the immediacy of the threat; and

(4) the danger to privacy and free expression posed by a full investigation.

Investigative Techniques

J. Whenever use of the following investigative techniques are permitted by these guidelines, they shall be implemented as limited herein:

(1) use of informants to gather information, when approved by FBI Headquarters, and subject to review at intervals not longer than 180 days; provided,

(a) when persons have been arrested or charged with a crime, and criminal proceedings are still pending, informants shall not be used to gather information concerning that crime from the person(s) charged; and

(b) informants shall not be used to obtain privileged information; and where such information is obtained by an informant on his own initiative no record or use shall be made of the information.

(2) "mail covers," pursuant to postal regulations, when approved by the Attorney General or his designee, initially or upon request for extension; and

(3) electronic surveillance in accordance with the requirement of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

Provided that whenever it becomes known that person(s) under surveillance are engaged in privileged conversation (e.g., with attorney), interception equipment shall be immediately shut off and the Justice Department advised as soon as practicable. Where such a conversation is recorded it shall not be transcribed, and a Department attorney shall determine if such conversation is privileged.

NOTE: These techniques have been the subject of strong concern. The committee is not yet satisfied that all sensitive areas have been covered (e.g., inquiries made under "pretext;" "trash covers," photographic or other surveillance techniques.)

III. TERMINATING INVESTIGATIONS

A. Preliminary, limited, and full investigations may be terminated at any time by the Attorney General, his designee, or FBI Headquarters.

B. FBI Headquarters shall periodically review the results of full investigations, and at such time as it appears that the standard for a full investigation under II(I) can no longer be satisfied and all logical leads have been exhausted or are not likely to be productive, FBI Headquarters shall terminate the full investigation.

C. The Department of Justice shall review the results of full domestic intelligence investigations at least annually, and shall determine in writing whether continued investigation is warranted. Full investigations shall not continue beyond one year without the written approval of the Department. However, in the absence of such notification the investigation may continue for an additional 30 day period pending response by the Department.

IV. REPORTING, DISSEMINATION, AND RETENTION

A. Reporting

1. Preliminary investigations which involve a 90-day extension under IIH and limited investigations under IIF, shall be reported periodically to the Department of Justice. Reports of preliminary and limited investigations shall include the identity of the subject of the investigation, the identity of the person interviewed or the person or place surveilled, and shall indicate which investigations involved a 90-day extension. FBI Headquarters shall maintain, and provide to the Department of Justice upon request, statistics on the number of preliminary investigations instituted by each field office, the number of limited investigations under IIF, the number of preliminary investigations that involved 90-day extensions under IIH, and the number of preliminary or limited investigations that resulted in the opening of a full investigation.

2. Upon opening a full domestic security investigation the FBI shall, within one week, advise the Attorney General or his designee thereof, setting forth the basis for undertaking the investigation.

3. The FBI shall report the progress of full domestic security investigations to the Department of Justice not later than 90 days after the initiation thereof, and the results at the end of each year the investigation continues.

4. Where the identity of the source of information is not disclosed in a domestic security report, an assessment of the reliability of the source shall be provided.

B. Dissemination

1. Other Federal Authorities

The FBI may disseminate facts or information obtained during a domestic security investigation to other federal authorities when such information:

(a) falls within their investigative jurisdiction;

(b) may assist in preventing the use of force or violence; or

79-064 O - 76 - 26

(c) may be required by statute, interagency agreement approved by the Attorney General, or Presidential directive. All such agreements and directives shall be published in the Federal Register.

2. State and Local Authorities

The FBI may disseminate facts or information relative to activities described in paragraph IB to state and local law enforcement authorities when such information:

(a) falls within their investigative jurisdiction;

(b) may assist in preventing the use of force or violence; or

(c) may protect the integrity of a law enforcement agency.

3. When information relating to serious crimes not covered by paragraph IA is obtained during a domestic security investigation, the FBI shall promptly refer the information to the appropriate lawful authorities if it is within the jurisdiction of state and local agencies.

4. Nothing in these guidelines shall limit the authority of the FBI to inform any individual(s) whose safety or property is directly threatened by planned force or violence, so that they may take appropriate protective safeguards.

5. The FBI shall maintain records, as required by law, of all disseminations made outside the Department of Justice, of information obtained during domestic security investigations.

C. Retention

1. The FBI shall, in accordance with a Records Retention Plan approved by the National Archives and Records Service, within _____ years after closing domestic service investigations, destroy all information obtained during the investigation, as well as all index references thereto, or transfer all information and index references to the National Archives and Records Service.

NOTE: We are not yet certain whether empirical data exists to help define a period of retention for information gathered in preliminary or full investigations. Whatever period is

determined should take into account the retention period for other categories of information (e.g., general criminal, organized crime, and background checks); since we have not yet considered these areas we cannot fix a period for retention at this time.

NOTE: It may also be possible to establish a sealing procedure to preserve investigative records for an interim period prior to destruction. After being sealed, access would be permitted only under controlled conditions.

2. Information relating to activities not covered by paragraph IA obtained during domestic security investigations, which may be maintained by the FBI under other parts of these guidelines, shall be retained in accordance with such other provisions.

3. The provisions of paragraphs one (1), and two (2) above apply to all domestic security investigations completed after the promulgation of these guidelines, and apply to investigations completed prior to promulgation of these guidelines when use of these files serves to identify them as subject to destruction or transfer to the National Archives and Records Service.

4. When an individual's request pursuant to law for access to FBI records identifies the records as being subject to destruction or transfer under paragraph one (1), the individual shall be furnished all information to which he is entitled prior to destruction or transfer.

WHITE HOUSE PERSONNEL SECURITY AND BACKGROUND INVESTIGATIONS

I. COLLECTION OF INFORMATION

A. Initiation of Investigation

1. White House investigations involving file reviews or field investigations conducted by the FBI shall be initiated only to ascertain facts and information relevant to the suitability of persons being considered for Presidential appointment; staff of the Executive Office; clearance for access to classified information; granting clearance for access to or service at the White House or other places under the protection of the U.S. Secret Service in connection with its duties to protect the President and the Vice President of the United States.

2. White House investigations involving file reviews or field investigations shall be initiated as follows:

   a. The President of the United States, and the Counsel or Associate Counsel to the President or the Attorney General may initiate investigations directly with the FBI.

   b. The Secretary of State and the Director of the National Security Counsel may request the FBI to conduct White House investigations when authorized by formal agreements with the Attorney General. These agreements shall designate by title all persons authorized to request White House inquiries, shall be consistent with the provisions of these guidelines, and are to be published in the Federal Register.

3. Requests for White House investigations involving file reviews shall be made or confirmed in writing; specify the official initiating the request; identify the person under investigation for appointment, clearance or service; and the purpose of the investigation as described in A(1) above.

4. Requests for White House investigations involving field investigations shall be made or confirmed in writing; specify the official initiating the investigation, and identify the person under investigation for appointment, clearance, or service. The request shall be accompanied by a statement signed by the subject of the investigation acknowledging that he has consented to the investigation with the knowledge that facts or information gathered shall be retained consistent with the FBI records retention plan. The requesting official must certify the subject of the investigation has been apprised of the provisions of Section (e)3 of the Privacy Act of 1974.

B. Investigation

1. White House investigations involving file reviews or field investigations must be thorough, precise, and fair.

2. Persons interviewed during White House field investigations shall be told that the individual under investigation is being considered for a position of trust involving the Government. The name of the official or agency initiating the investigation, or the position for which the individual is being considered shall not be disclosed unless specifically authorized by the requesting official.

3. Subject to the Freedom of Information Act and Privacy Act of 1974, persons interviewed during White House field investigations may be assured that, to the extent permitted by law, information identifying such persons will be kept confidential.

4. Where a person is the subject of a subsequent White House field investigation, information contained in the earlier report reflecting adversely on the person shall be re-investigated, where such inquiry is likely to yield information relevant to the current investigation and where such inquiry is practicable.

C. Reporting

1. Information obtained during White House file reviews or field investigations shall be furnished to the initiating authority and/or the White House. The FBI shall retain a record of persons to whom such information is furnished.

2. Any investigative efforts to determine the truth or falsity of reported derogatory allegations or information shall be reported.

3. Where the identity of the source of information is not reported in a White House file review or field investigation, an assessment shall be provided of the reliability of such source.

II. DISSEMINATION AND RETENTION OF INFORMATION

A. Retrieval

1. The FBI shall retain a record of all relevant information gathered during the course of White House investigations consistent with these guidelines.

2. Information obtained during these investigations may be indexed in such a manner as to assist in its subsequent retrieval.

B. Access

1. The Director of the FBI shall insure that access to White House investigative files under his control is restricted and that stringent controls are maintained over such files limiting their use to official purpose.

2. Officials outside the FBI to whom White House file review and field investigations reports are furnished shall insure that internal access thereto is restricted to persons directly involved in making Presidential appointments; determining Executive Office staffing; granting clearance to classified information; approving access to or service at the White House or other place under the protection of the U.S. Secret Service as described in these guidelines. A record shall be maintained of the identity and organizational unit of officials requesting access to White House investigative files, as well as the dates these files are issued and returned.

C. Dissemination

1. Where during the couse of a White House field investigation the FBI finds some indication that the person under investigation may have committed a crime or other violation of law the FBI shall notify the initiating official thereof; and either investigate the crime if within its jurisdiction or refer the facts or information of the possible violation to appropriate authorities for determination.

2. No subsequent dissemination shall be made by the FBI of the results of White House field investigations or file reviews, conducted for the incumbent Administration, without the express approval of the President, Counsel, or Associate Counsel to the President, except as expressly required by federal statute or as part of an investigation of a violation of law.

3. No one receiving FBI reports of White House file reviews or field investigations shall reproduce or disseminate these materials other than in accord with B(2) above without the express consent of the FBI. Such dissemination must be predicated upon the request of an official authorized by or in accordance with these guidelines to initiate a White House investigation, and only for a purpose authorized by these guidelines.

4. The FBI and officials receiving reports of White House file reviews or field investigations shall maintain a record of all dissemination of these materials to other agencies.

D. Retention of Information

1. Information obtained during White House file reviews or field investigations shall be retained at FBI Headquarters and at FBI field offices as prescribed by the FBI Records Retention Plan.

2. Results of White House investigations maintained by the FBI shall be destroyed _____ years after completion of the investigation subject to the following conditions:

   a. files and information determined by the Archivist of the United States to be of historic interest shall be transferred to

the custody of the National Archives and Records Service _____ years after the completion of the investigation.

b. files and information relating to persons who have been re-investigated may be retained _____ years from the date of the latest investigation.

3. Anyone receiving FBI reports of White House file reviews or field investigations shall destroy such reports within ninety (90) days after receiving them, unless notice in writing is given to the FBI that an additional period of time, not exceeding ninety (90) days, is needed to complete a decision relating to the White House investigation.

4. The provisions of paragraphs two (2) and three (3) above apply to all inquiries completed after the promulgation of these guidelines. The provisions of paragraph two (2) apply to inquiries completed prior to promulgation of these guidelines when use of these files serves to identify them as subject to destruction or transfer to the National Archives and Records Service.

5. When an individual's request pursuant to law for access to files pertaining to him identifies files as being subject to destruction or transfer under paragraph two (2), he shall be furnished all information to which he is entitled prior to destruction or transfer.

NOTE: The primary reference of "pursuant to law" in this paragraph is to the Privacy Act of 1974, which specifically authorizes access to background investigation files.

REPORTING ON CIVIL DISORDERS AND DEMONSTRATIONS
INVOLVING A FEDERAL INTEREST

I. Basis for Reports and Investigations

The Federal Bureau of Investigation is responsible for reporting information on civil disturbances or demonstrations in four categories:

A. Investigating --

1) violations of federal criminal law directed explicitly at civil disorders (e.g. 18 U.S.C. 231, 2101); and

2) violations of federal criminal law of general applicability occuring during civil disorders.

B. Providing information and assistance, upon request of the Secret Service, to aid in carrying out its protective responsibilities under 18 U.S.C. 112, 970, 3056 and P.L. 90-331.

NOTE: Under 18 U.S.C. 112 and 3056 the Secret Service is assigned responsibility to provide protection to certain U.S. Government officials and foreign officials and visitors. P.L. 90-331 provides Secret Service protection for candidates for office and authorizes Secret Service to call on any federal agency to assist in this regard. Responsibility for protection of foreign missions is assigned to the Executive Protection Service under the direction of the Secret Service. This accounts for the reference to 18 U.S.C. 970 dealing with damage to foreign missions.

C. Providing information concerning actual or threatened civil disorders which may require the presence of federal troops to enforce federal law or federal court orders (10 U.S.C. 332, 333) or which may result in a request by State authorities to provide federal troops in order to restore order (10 U.S.C. 331).

NOTE: The statutes cited provide three bases for the use of troops in connection with civil disorders. Section 332 authorizes troops, at Presidential initiative, to enforce federal law and was the basis for the use of troops to protect the mail in the Pullman strike. Section 333 deals with the use of troops to protect civil rights and enforce court orders and was the basis for using troops at Little Rock and Oxford. Section 331 permits the President to send troops at the request of a State when State authorities cannot restore order, e.g. the Detroit Riot.

D. Providing information relating to demonstration activities which are likely to require the federal government to take action to facilitate the activities and provide public health and safety measures with respect to those activities.

NOTE: While there is no specific statutory authority for collection of information in these circumstances, the Second Circuit recognized in Fifth Avenue Peace Parade Committee v. Kelley, 480 F.2d 326, cert. denied, 415 U.S. 948, that the federal government has a legitimate need for information concerning demonstrations planned at federal facilities in order to provide services in connection with the demonstration. For example, considerable information was needed in order to fashion an appropriate permit for the November 1971 moratorium march in Washington, D.C.

II. Criminal Offenses

A. Investigation of criminal offenses referred to in paragraph I.A. shall be undertaken in the manner provided for in guidelines relating to criminal investigations generally.

B. Information concerning criminal offenses within the investigative jurisdiction of the FBI which is acquired incidentally in the course of implementing parts III through V, shall be handled in the manner provided for in guidelines relating to criminal investigations generally.

C. Information concerning criminal offenses within the investigative jurisdiction of another federal agency which is acquired incidentally in the course of implementing parts II through V, shall be reported to the agency having jurisdiction.

D. Information concerning serious criminal offenses within the investigative jurisdiction of State or local agencies which is acquired incidentally in the course of implementing parts II through V shall be reported to the appropriate lawful authorities.

NOTE: Using the criteria now applied by NCIC, the reference to serious offenses would exclude such matters as: drunkeness, vagrancy, loitering, disturbing the peace, disorderly conduct, adultery, fornication, and consensual homosexual acts, false fire alarm, non-specific charges of suspicion or investigation, traffic violations, and juvenile delinquency.

E. Information relating to criminal offenses acquired in the course of implementing parts II through V shall be retained and indexed as provided for in guidelines relating to criminal investigations generally.

III. Assisting the Secret Service

A. Information relating to the protective responsibilities of the Secret Service described in Paragraph I.B, which is acquired incidentally by the FBI in the course of carrying out its responsibilities, shall be reported to the Secret Service. The FBI shall not undertake specific investigations for the purpose of assisting the Secret Service in its protective responsibilities without a specific request from the Director of the Secret Service or his designee, made or confirmed in writing.

NOTE: The Department should undertake to review with the Secret Service existing agreements on the dissemination of information from the FBI to the Secret Service. The draft report of the General Accounting Office indicates that very little information reported by the FBI is actually retained by Secret Service.

B. A record shall be made of all information reported to the Secret Service pursuant to paragraph III.A. and the record shall be retained by the FBI for five years.

NOTE: This is the standard Privacy Act accounting requirement.

C. Information reported to the Secret Service may be retained by the FBI for a period of ____ years.

NOTE: The retention period for this information will be considered in a general review of retention under all the guidelines.

IV. Civil Disorders

A. Information relating to actual or threatened civil disorders acquired by the FBI from public officials or other public sources or in the course of its other investigations, shall be reported to the Department of Justice.

B. The FBI shall not undertake investigations to collect information relating to actual or threatened civil disorders except upon specific request of the Attorney General or his designee. Investigations will be authorized only for a period of 30 days but the authorization may be renewed, in writing, for subsequent periods of 30 days.

C. Information shall be collected and reported pursuant to paragraphs A and B above for the limited purpose of assisting the President in determining whether federal troops are required and determining how a decision to commit troops shall be implemented. The information shall be based on such factors as:

1) The size of the actual or threatened disorder -- both in number of people involved or affected and in geographic area;

2) The potential for violence;

3) The potential for expansion of the disorder in light of community conditions and underlying causes of the disorder;

4) The relationship of the actual or threatened disorder to the enforcement of federal laws or court orders and the likelihood that State or local authorities will assist in enforcing those laws or orders;

5) The extent of State or local resources available to handle the disorder.

D. Investigations undertaken, at the request of the Attorney General or his designee, to collect information relating to actual or threatened civil disorders shall be limited to inquiries of:

1) FBI files and indices;

2) Public records and other public sources of information;

3) Federal, State and local records and officials;

4) Established informants or other established sources of information.

Interviews of individuals other than those listed above, and physical or photographic surveillance shall not be undertaken as part of such an investigation except when expressly authorized by the Attorney General or his designee.

E. Information relating to civil disorders, described in paragraph C above, shall be reported to the Department of Justice and may also be reported to federal, state or local officials at the location of the actual or threatened disorder who have a need for the information in order to carry out their official responsibilities in connection with such a disorder.

F. Information acquired or collected pursuant to paragraphs A through D above may be retained by the FBI for a period of _____ years but may not be indexed in a manner which permits retrieval of information by reference to a specific individual unless the individual himself is the subject of an authorized law enforcement investigation.

described in paragraph C. Such information shall be collected only by inquiries of:

1) FBI files and indices,

2) Public records and other public sources of information,

3) Federal, state and local records and officials,

4) Persons involved in the planning of the demonstration, provided that in conducting interviews with such persons the FBI shall initially advise them specifically of the authority to make the inquiry and the limited purpose for which it is made.

E. The FBI shall not undertake to photograph any demonstration or the preparation therefor in carrying out its responsibilities under paragraph V.

F. Information acquired or collected pursuant to paragraphs A through D above may be retained by the FBI for a period of ____ years but may not be indexed in a manner which permits identification of an individual with a particular demonstration or retrieval of information by reference to a specific individual, unless the individual himself is the subject of an authorized law enforcement investigation.

NOTE: Retention period to be fixed later; indexing limit to be implemented immediately.

NOTE: Retention period to be fixed later; indexing limit to be implemented immediately.

V. Public Demonstrations

A. Information relating to demonstration activities which are likely to require the federal government to take action to facilitate the activities and provide public health and safety measures with respect to those activities, which is acquired incidentally by the FBI in the course of carrying out its responsibilities, shall be reported to the Department of Justice.

B. The FBI shall not undertake investigations to collect information with respect to such demonstrations except upon specific request of the Attorney General or his designee.

C. Information collected and reported pursuant to paragraphs A and B above shall be limited to that which is necessary to determine:

1) The date, time, place and type of activities planned;

2) The number of persons expected to participate;

3) The intended mode of transportation to the intended site or sites and the intended routes of travel;

4) The date of arrival in the vicinity of the intended site and housing plans, if pertinent;

5) Similar information necessary to provide an adequate federal response to insure public health and safety and the protection of First Amendment rights.

NOTE: Clause 5 above is intented to encompass such additional facts affecting the federal responsibility as unusual health needs of participants, counter-demonstrations planned which may increase safety needs, or possible inability of participants to arrange return transportation.

D. Investigations undertaken to collect information relating to demonstrations pursuant to paragraph B above shall be limited to determining the information

described in paragraph C. Such information shall be collected only by inquiries of:

1) FBI files and indices,

2) Public records and other public sources of information,

3) Federal, state and local records and officials,

4) Persons involved in the planning of the demonstration, provided that in conducting interviews with such persons the FBI shall initially advise them specifically of the authority to make the inquiry and the limited purpose for which it is made.

E. The FBI shall not undertake to photograph any demonstration or the preparation therefor in carrying out its responsibilities under paragraph V.

F. Information acquired or collected pursuant to paragraphs A through D above may be retained by the FBI for a period of ____ years but may not be indexed in a manner which permits identification of an individual with a particular demonstration or retrieval of information by reference to a specific individual, unless the individual himself is the subject of an authorized law enforcement investigation.

NOTE: Retention period to be fixed later; indexing limit to be implemented immediately.

U.S. Department of Justice. Memorandum for the Attorney General--Subject: Electronic Surveillance,and National Security Electronic Surveillance History, Policy and Procedure (Memoranda from William Olson to Elliott Richardson). U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure and Subcommittee on Constitutional Rights. Committee on Foreign Relations. Subcommittee on Surveillance. Warrantless wiretapping and electronic surveillance--1974. Joint hearings, 93th Congress, 2d session. April 3-May 23, 1974. pp. 18-39.

[Memorandum from William Olson, former Assistant Attorney General for Internal Security to Elliot Richardson, former U.S. Attorney General, June 1973]

MEMORANDUM FOR: THE ATTORNEY GENERAL—SUBJECT: ELECTRONIC SURVEILLANCE

In recent days considerable confusion has arisen about the subject of electronic surveillance. The following is a summary of the various types of electronic surveillance currently utilized in the Department of Justice including a discussion of the legal basis of and the procedures employed for each.

Preliminarily, the term electronic surveillance is a broad and often misunderstood term. As used by the Department it includes both telephone surveillance (sometimes referred to as either wiretap or technical surveillance) and microphone surveillance (sometimes referred to as either bug or electronic listening device).

I. NATIONAL SECURITY ELECTRONIC SURVEILLANCE

A. Legal Basis

The concept of national security electronic surveillance is generally conceded to have originated with the May 21st, 1940, memorandum from President Franklin D. Roosevelt to Attorney General Jackson, which memorandum stated in part:

"You are therefore authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigating agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the government of the United States, including suspected spies."

The President's power to employ electronic surveillance in national security matters has been justified in aid of his constitutional powers to provide for the defense of the nation and to conduct its foreign affairs. Over the years such electronic surveillance has been employed to obtain intelligence information rather than for the purpose of obtaining evidence for prosecution. From at least 1946 until a decision in the *Keith* case in June of 1972, every president and attorney general have authorized the use of such surveillance in both foreign and domestic security matters. On June 19, 1972, the Supreme Court decided the *Keith* case (*United States* v. *United States District Court*, 407 USC 297) and in doing so held that the Fourth Amendment (which shields private speech from unreasonable surveillance) requires prior judicial approval for the type of *domestic security surveillance involved in that case*. The Court made no judgment as to the constitutionality of national security electronic surveillance to gather foreign intelligence information. However, every lower court that has considered this question has sustained the government's position.

B. Procedures

National security electronic surveillance has always been conducted only by the Federal Bureau of Investigation and with the approval of the Attorney General on behalf of the President. Prior to March 1965 national security microphone surveillance was utilized upon the authorization of the Director of the Federal Bureau of Investigation under a general authority from the Attorney General. Since March 1965 all national security electronic surveillance has been utilized only after the written approval of the Attorney General.

Current procedures require that all requests for authorization of a national security electronic surveillance be made in writing by the Director of the Federal Bureau of Investigation to the Attorney General on behalf of the President. In some instances other federal governmental agencies may request use of national security electronic surveillance but such requests are made to the Director of the Federal Bureau of Investigation who in turn formally requests such surveillance of the Attorney General. Each such request is considered by the Attorney General in conjunction with all intelligence information available to the executive branch of the government which bears upon the request. Up until the *Keith* decision it was necessary for the proposed surveillance to satisfy one or more of the following criteria: (1) that it is necessary to protect the nation against actual or potential attack or any other hostile action of a foreign power; (2) that it is necessary to obtain foreign intelligence information deemed essential to the security of the United States; (3) that it is necessary to protect national security information against foreign intelligence activities; (4) that it is necessary to protect the United States against the overthrow of the Government by force or other unlawful means; and (5) that it is necessary to protect the United States against a clear or present danger to the structure or the existence of its Government.

After the *Keith* decision only the first three criteria (dealing with the foreign aspects of national security) have been taken into consideration. These criteria reflect the standards enunciated in 18 USC 2511(3) enacted by the Omnibus Crime Control and Safe Streets Act of 1968. In those cases where a determination is made that one or more of the appropriate standards is met a written authorization for a specified period not to exceed three months is executed by the Attorney General.

II. ELECTRONIC SURVEILLANCE UNDER TITLE III OF OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968

A. Legal Basis

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which was signed by President Johnson on June 19, 1968, established a comprehensive scheme for controlling the interception of wire and oral communications (wiretapping and bugging). In brief the provisions of Title III prohibit, with certain limited exceptions, the interception of wire or oral communications by means of electronic or mechanical devices by all persons other than duly authorized law enforcement officials engaged in the investigation of specified types of major crimes after obtaining a court order based upon probable cause.

Authorized by Congress in June 1968, the Title III authority nevertheless was not employed until February 1969, shortly after Attorney General Mitchell took office.

B. *Procedures*

Under the statute, every application for a court order must be approved by the Attorney General or by an Assistant Attorney General specifically designated by him. Requests for such applications are made to the Attorney General by the head of the agency having investigative jurisdiction of the offense for which the application is sought, such as the FBI, the Bureau of Narcotics and Dangerous Drugs, Secret Service, Customs Service, IRS, Postal Service, etc.

After approval by the Attorney General, based upon a showing of probable cause to believe that an offense specified in the statute is being committed, a written, sworn application supported by affidavit of an investigative agent is submitted to a Federal Court requesting issuance of an order authorizing interception of wire or oral communications over a particular telephone or from particular premises. Upon a requisite showing of probable cause and a finding that normal investigative techniques have been unsuccessful, the Court issues an order authorizing interception for a specified period of time, or until the objective is achieved, which by statute cannot exceed thirty days. Extensions of a court order may be obtained under the same conditions as an original order upon an additional showing of probable cause and that the objective has not yet been achieved. Any electronic surveillance authorized by the court order is conducted by the particular agency which had investigative jurisdiction of the offense.

To date, the majority of court authorized interceptions have been conducted in connection with Federal gambling offenses, narcotics violations and extortion offenses. Other court authorized interceptions have been conducted in connection with such offenses as kidnaping, counterfeiting, theft from interstate shipment, obstruction of justice, bribery, interstate transportation of stolen property and racketeer influenced and corrupt organizations.

III. CONSENSUAL ELECTRONIC SURVEILLANCE

A. *Legal Basis*

The electronic monitoring of a conversation with the consent of one but not all of the participants is not subject to the same stringent requirements which apply to the interception of private communications. Such electronic surveillance includes both the monitoring of telephone conversations and the use of recording and transmitting devices. Such electronic surveillance was specifically excepted from the coverage of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (subsection 2511(2) of Title 18 of the United States Code), and was further upheld by the Supreme Court in *United States* v. *White*, 401 U.S. 745 (1971).

B. Procedures

Although it is clear that such monitoring is constitutionally and statutorily permissible, and is a necessary investigative technique not only in the securing of corroborative evidence but frequently as a protection to the physical safety of government agents, the Department of Justice recognizes that careful self-regulation of its use by the Executive branch of the government is desirable. In accordance with internal regulation, the Department of Justice supervises and maintains records of all instances in which such consensual monitoring is undertaken by investigative bureaus of the Department and by other executive agencies. In all cases involving the use of recording or transmitting devices the agency must either secure the advance approval of the Attorney General, or, if exigent circumstances—such as the imminent loss of essential evidence or a threat to the safety of an agent—preclude advance authorization, must promptly notify the Attorney General of the use. In cases involving the consensual monitoring of telephone conversations the advance approval or subsequent notification of the Attorney General is not required.

[Memorandum from William Olson to Elliot Richardson]

NATIONAL SECURITY ELECTRONIC SURVEILLANCE HISTORY, POLICY AND PROCEDURE 1924–73

This document is intended to set forth the historical experience of the Department of Justice with wiretapping in the national security area, including the period following the enactment of Title III of Public Law 90–351. Although the

21

practice that is popularly known as "national security wiretapping", which refers to the conduct of electronic surveillance authorized by the Attorney General as necessary to gather intelligence information to preserve the national security, had its inception in 1940, a proper analysis of the practice requires an understanding of the historical experience of the Department with all forms of electronic surveillance.

At the outset, it should be made clear that electronic surveillance is a broad, and often misunderstood, term. As used by the Department, it can refer to both telephone surveillance ("wiretap or technical surveillance") and microphone surveillance ("bug or electronic listening device"). The unwary, or the uninformed, have often confused or combined these two separate categories of electronic surveillance, with misleading results. In the presentation which follows, these terms will be used as the Department presently defines them, and the development of policies within the Department on these types of surveillance until 1968 will be explained separately. As will become apparent, officials within the Department itself have not always appreciated the distinction between the two categories.

I. TELEPHONE SURVEILLANCE

Prior to 1940

In the period immediately following World War I, wiretapping or telephone surveillance played an important role in helping to ferret out prohibition law violators. This investigative technique was employed in such cases by the Bureau of Prohibition which, at this time, was part of the Department of the Treasury. However, Attorney General Harlan Fiske Stone, in 1924, prohibited such activity by personnel of the Department of Justice. In keeping with this prohibition, the Director of the Bureau of Investigation (the original name of the Federal Bureau of Investigation), which was a part of the Department of Justice, with the approval of Attorney General John G. Sargent, included the following section in the Bureau's *Manual of Rules and Regulations*, issued on March 1, 1928:

> Unethical tactics: Wiretapping, entrapment, or the use of any other improper, illegal or unethical tactics in procuring information in connection with investigative activity will not be tolerated by the Bureau.

In June of that year, the Supreme Court rendered its decision in *Olmstead v. United States*, 277 U.S. 438 (1928), which involved a prosecution for conspiracy to violate the National Prohibition Act, in which much of the Government's evidence had been obtained by the use of wiretapping. The Court held that the evidence was admissible and that the wiretapping was not unconstitutional, because the Fourth Amendment's protections did not apply to the seizure of conversations, and the installation and conduct of the wiretaps in question had not involved physical intrusions, or trespass, upon any property of the defendants. Nevertheless, the Department of Justice, and its Bureau of Investigation retained its prohibition on wiretapping until 1931.

In 1930, the Bureau of Prohibition was transferred from the Department of the Treasury to the Department of Justice. This transfer created a problem which Attorney General William B. Mitchell summarized in a January 19, 1931 memorandum, to which he later that year referred in his testimony before the House Committee on Expenditures in the Executive Departments:

"Of course, the present condition in the Department cannot continue. We cannot have one Bureau in which wiretapping is allowed and another in which it is prohibited. The same regulations must apply to all . . . . I think I should give a direction applicable to all bureaus and divisions of the Department that no tapping of wires should be permitted by any agent of the Department without the personal direction of the chief of the bureau involved, after consultation with the Assistant Attorney General in charge of the case."

Subsequent to this testimony, the Director of the Bureau of Investigation, at the direction of Attorney General Mitchell, changed the regulation dealing with wiretapping to read as follows:

"Wiretapping: Telephone or telegraph wires shall not be tapped unless prior authorization of the Director of the Bureau has been secured."

Also at the request of the Attorney General, instructions were issued that no wiretap was to be instituted without the written approval of the Assistant Attorney General in charge of the particular case.

From the date of the issuance of that regulation on February 19, 1931 until 1940, wiretapping was authorized "only in those cases involving the safety of victims of kidnappings, the location and apprehension of desperate criminals, and in espionage and sabotage and other cases considered to be of major law enforcement importance."

Meanwhile, in June 1934, the Congress enacted Section 605 of the Federal Communications Act of 1934, 47 U.S.C. 605, which made it a crime for "any person" to intercept, without authorization, and divulge or publish the contents of wire and radio communications. This section was judicially construed by the Supreme Court in December 1937 in *Nardone* v. *United States*, 302 U.S. 379. The Court ruled that Congress did intend to include Federal agents within the operation of the statute and to preclude the receipt as evidence in judicial proceedings of intercepted conversations. Elaborating on this decision in *Nardone* v. *United States*, 308 U.S. 338 (1939), the Supreme Court held that Section 605 barred not only the use of evidence of intercepted conversations themselves, but also the use of evidence shown to be derived therefrom.

The Department construed these decisions as not prohibiting the interception of wire communications *per se*, but only the *interception and the divulgence* of their contents. The Department continued to authorize wiretapping, although it recognized that nothing obtained therefrom could be used as evidence. This situation continued until 1940.

1940 to 1968

On March 15, 1940, Attorney General Robert H. Jackson, by Order No. 3343, rescinded the provision of the *Manual of Rules and Regulations* of the Federal Bureau of Investigation, adopted in 1931, with respect to wiretapping, and briefly reinstated the prohibition in effect prior thereto. Less than three months later, however, on May 21, 1940, President Franklin D. Roosevelt, in a memorandum to Attorney General Jackson stated that he was convinced that the Supreme Court never intended to have its ruling concerning wiretaps apply to grave matters involving the defense of the nation. The President then directed the Attorney General to employ wiretaps in cases involving subversive activities against the Government, including suspected spies, but subject to the Attorney General's approval. (See Appendix A).

In support of this practice, in an October 6, 1941 memorandum, Assistant Solicitor General Charles Fahy offered the then Attorney General, Francis Biddle, his legal opinion that the Attorney General had authority to authorize wiretapping and that 47 U.S.C. 605 did not apply to divulgence to the President, or someone acting in his behalf, of intercepted information relating to the security of the nation. Attorney General Biddle endorsed this opinion in a memorandum to FBI Director J. Edgar Hoover on October 9, 1941. (See Appendix B).

On June 17, 1946, this policy was specifically continued in force when President Truman personally approved a memorandum from Attorney General Tom Clark, in which the Attorney General restated President Roosevelt's 1940 directive and expressed his view that the policy should remain in effect and that it was imperative that the investigative measures referred to be employed "in cases vitally affecting the domestic security, or where human life is in jeopardy." (See Appendix C).

This policy was further continued when Attorney General McGrath wrote in a February 26, 1952 memorandum to the Director of the Federal Bureau of Investigation:

". . . As you state, the use of wiretapping is indispensable in intelligence coverage of matters relating to espionage, sabotage, and related security fields. Consequently, I do not intend to alter the existing policy that wiretapping surveillance should be used under the present highly restricted basis and when specifically authorized by me."

Subsequently, in 1955, Attorney General Herbert Brownell stated that he did not believe it necessary to obtain further approval of the existing practice from President Eisenhower as he was of the opinion that President Roosevelt's approval was sufficient. (Appendix D).

Despite intervening Presidential and Attorney General directives to the contrary, it was not until March 13, 1962 that Attorney General Robert H. Jackson's March 15, 1940 regulation prohibiting wiretapping was formally rescinded. On that date, Attorney General Robert F. Kennedy issued Order No. 263–62 which amended Attorney General Jackson's Order No. 3343 of March 15, 1940. Attorney General Kennedy stated at that time that the amendment was necessary "in order to reflect the practice which had been in effect since May 21, 1940." The order further provided "Existing instructions to the Federal Bureau of Investigation with respect to obtaining the approval of the Attorney General for wiretapping are continued in force." (Appendix E).

Finally, in a memorandum to the heads of all Executive Departments and Agencies dated June 30, 1965, President Lyndon Johnson directed that there

be no further nonconsensual interception of telephone communications by Federal personnel within the United States "except in connection with investigations related to the national security", and then only after first obtaining the written approval of the Attorney General. (See Appendix F.) This policy for the authorization of telephone surveillance in national security cases was continued in the Justice Department until the adoption of the Omnibus Crime Control and Safe Streets Act of 1968, which became effective on May 19 of that year. The policies of the Department in this area since that date will be explained below.

II. MICROPHONE SURVEILLANCE

The records of the Department of Justice with respect to the historical development of microphone surveillance policy are, unfortunately, not as complete as is the case with telephone surveillance, and it is very difficult to find evidence of a Departmental position on this subject over the years. In fact, explicit treatment of microphone surveillance as a separate category raising distinct legal questions is not reflected in Departmental records until the early 1950's.

Several factors may have contributed to this situation. For one, the legal status of microphone surveillance was far from settled. Although the Supreme Court's decision in *Olmstead* had intimated that a microphone surveillance which involved a trespass in its installation might violate the Fourth Amendment, it did not so hold and the case involved a wiretap and not a microphone surveillance. Similarly, microphone surveillance was not prohibited by Section 605 of the Communications Act of 1934, which applied only to wire communications, although that statute left open the question whether it forbade the divulgence of conversations which a microphone surveillance overheard but did not "intercept"—a question not answered until the Supreme Court decided the *Goldman* case, *infra*, in 1942. Another contributing factor was the fact that President Roosevelt's memorandum in 1940 was apparently limited to wiretapping.

During the period of 1931 to 1940, it appears safe to assume that microphone surveillances were utilized under the same standards as telephone surveillances—"in those cases involving the safety of victims of kidnapping, the location and apprehension of desperate criminals, and in espionage, sabotage and other cases considered to be of major law enforcement importance."

In 1942, the Supreme Court decided *Goldman* v. *United States*, 316 U.S. 129, a case in which Federal agents had overheard certain telephone conversations conducted in the defendant's office through a microphone surveillance by placing a "detectaphone" on the outside of the office wall. The Court held that 47 U.S.C. 605 had not been violated and neither had the Fourth Amendment, as the use of the device had not involved a trespass into the office in question. Thus, as of the date of the *Goldman* decision, the test for the validity of a microphone surveillance was established to be whether or not it involved a trespass.

The *Goldman* case arose in a setting in which the Government attempted to introduce in evidence the microphone overhearings resulting from electronic surveillance in a *criminal investigation*. At the time of *Goldman*, the use of electronic surveillance for *national security intelligence* purposes had never been questioned by the courts. As a result of *Goldman* and subsequent court decisions expanding and defining the trespass concept, a distinction gradually arose in the Department between the intelligence gathering function as opposed to the function of obtaining evidence for prosecutive purposes. In the case of wiretapping, this distinction already existed in the Department of Justice as a result of the enactment of the Communications Act of 1934 and the national security exception enunciated in the memorandum of President Roosevelt of May 21, 1940. Thus microphone surveillances came to be utilized in some organized crime matters as well as in national security cases even though trespass was involved to obtain intelligence information as opposed to obtaining evidence for prosecution.

In a memorandum to Attorney General McGrath dated October 6, 1951, the Director of the Federal Bureau of Investigation summarized the existing policy on microphone surveillance:

> As you are aware, this Bureau has also employed the use of microphone installations on a highly restrictive basis, chiefly to obtain intelligence information. The information obtained from microphones, as in the case of wire taps, is not admissible in evidence. In certain instances it has been possible to install microphones without trespass, as reflected by opinions rendered in the past by the Department on this subject matter. In these instances the information obtained, of course, is treated as evidence and therefore is not regarded as purely intelligence information.

Subsequently, in the February 26, 1952 memorandum to the Director of the FBI discussed *supra*, Attorney General McGrath expressed the opinion that: "The use of microphone surveillance which does not involve trespass would seem to be permissible under the present state of the law." In a March 4, 1952 internal memorandum, the Director of the Federal Bureau of Investigation declared that he would not authorize microphone surveillances in cases involving trespass. (Appendix G).

In 1954, the Supreme Court decided the case of *Irvine* v. *California*, 347 U.S. 128, in which State authorities had obtained evidence of defendant's illegal gambling activities by installation of a microphone in his bedroom. The effect of this decision on Federal policy was discussed in a May 20, 1954 memorandum from Attorney General Herbert Brownell to the Director of the Federal Bureau of Investigation. (Appendix H). In this memorandum, the Attorney General underscored the "intelligence function [of the FBI] in connection with internal security matters", and noted that, while microphone surveillances were generally restricted to situations where no trespass was involved, there might arise situations where considerations of national security dictated the use of microphone surveillance even though it involved trespass and even in situations such as had been involved in *Irvine*. Attorney General Brownell concluded:

"I recognize that for the FBI to fulfill its important intelligence function, considerations of internal security and the national safety are paramount and, therefore, may compel the unrestricted use of this technique in the national interest."

On May 4, 1961, the Director of the FBI, in a memorandum to Deputy Attorney General Byron R. White (Appendix I), informed him that:

"Our policy on the use of microphone surveillances is based upon a memorandum from former Attorney General Brownell dated May 20, 1954, in which he approved the use of microphone surveillances with or without trespass."

This memorandum quoted the passage from the Brownell memorandum set forth *supra*, and noted that microphone surveillances involving trespass were being employed in important organized crime investigations, as well as in the internal security field.

Prior to March of 1965, Department policy did not require the Attorney General's authorization of microphone surveillances which involved trespass, as had been the case with telephone surveillance since 1940. Available Department records do indicate instances where the personal authorization of the Attorney General was sought for microphone surveillances involving trespass, but there is no indication of a consistent Departmental policy to this effect. However, in March of 1965, Attorney General Katzenbach instituted the requirement that all microphone installations receive the prior authorization of the Attorney General. Since that time, Department policy has required the prior approval of the Attorney General for both microphone and telephone surveillance. At the same time, Attorney General Katzenbach instituted a new policy that microphone and telephone surveillances would be authorized only for six-month periods at a time, and that each extension of a surveillance must receive a new authorization. This evolution of microphone surveillance policy was summarized by Solicitor General Thurgood Marshall in a "Supplemental Memorandum for the United States", submitted to the Supreme Court on July 13, 1966, in connection with the case of Fred Black:

> Under Department practice in effect for a period of years prior to 1963, and continuing into 1965, the Director of the Federal Bureau of Investigation was given authority to approve the installation of devices such as that in question for intelligence (and not evidentiary) purposes when required in the interest of internal security or national safety, including organized crime, kidnappings and matters wherein human life might be at stake. Acting on the basis of the aforementioned Departmental authorization, the Director approved installation of the device involved in the instant case.

As regards the policies of agencies other than the Department of Justice, President Johnson's memorandum of June 30, 1965, as noted earlier, banned all wiretapping, except where it had been approved in national security cases by the Attorney General. On the subject of non-telephone conversations, the memorandum contains the following language:

> Utilization of mechanical or electronic devices to overhear non-telephone conversations is an even more difficult problem, which raises substantial and unresolved questions of Constitutional interpretation. I desire that each agency conducting such investigations consult with the Attorney General to ascertain whether the agency's practices are fully in accord with the law and with a decent regard for the rights of others.

Departmental policy in the light of this Presidential directive was enunciated in a paragraph set forth in the *Black* memorandum, *supra*, and communicated to all United States Attorneys in a November 3, 1966 memorandum from Attorney General Ramsey Clark:

> Present practice, adopted in July 1965 in conformity with the policies declared by President Johnson on June 30, 1965 for the entire Federal establishment, prohibits the installation of listening devices in private areas (as well as the interception of telephone and other wire communications) in all instances other than those involving the collection of intelligence affecting the national security.

III. CURRENT ELECTRONIC SURVEILLANCE POLICY

As noted, Departmental policy on the conduct of telephone surveillance and microphone surveillance since 1965 has been the same—that it may be conducted for intelligence purposes where the Attorney General has approved it as required by the interests of national security. In the meantime, however, the law relating to electronic surveillance was being significantly transformed.

In two major decisions in the same term, *Berger* v. *New York*, 388 U.S. 41 (1967) and *Katz* v. *United States*, 389 U.S. 347 (1967), the Supreme Court overruled *Olmstead* and held that the Fourth Amendment did apply to searches and seizures of conversations and protected all conversations of an individual as to which he has a reasonable expectation of privacy. However, the Court in *Katz* did specifically leave undecided this question:

> ... whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security. 389 U.S. at 358, n. 23.

In response to these decisions, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510 *et seq.*, P.L. 90–351.

On June 19, 1972, the Supreme Court decided the *Keith* case (*United States* v. *United States District Court*, 407 U.S. 297 (1972)) and in doing so held that "the Fourth Amendment (which shields private speech from unreasonable surveillance) requires prior judicial approval for the type of *domestic security surveillance* involved in that case. The Court carefully pointed out that it was only condemning warrantless electronic surveillance directed at a "domestic organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies."

The Court made no judgment as to the constitutionality of national security electronic surveillance to gather foreign intelligence information. However, every lower court that has considered this question has sustained the Government's position. At the district court level, the Government has prevailed in: *United States* v. *Dellinger, et al.*, N.D. Ill., No. 69 CR 180; *United States* v. *Butenko and Ivanov*, D.N.J., No. 418–63; *United States* v. *Stone*, 305 F. Supp. 75 (D.C. D.C., 1969); *United States* v. *O'Baugh*, 304 F. Supp. 767 (D.C. D.C., 1969); *United States* v. *Enten*, D.C. D.C., Crim. No. 166–71; *United States* v. *Hoffman*, D.C. D.C., Crim. No 973–71 Also see dictum in *United States* v. *Smith*, 321 F. Supp. 424, 425–426 (1971). In the only appellate test to date the Fifth Circuit found such surveillances constitutional in *United States* v. *Clay*, 430 F. 2d 165 (5th Cir. 1970), reversed on other grounds, 403 U.S. 698.

Since the enactment of Title III of the 1968 Act, the Department of Justice has adhered to the position that only to approve the conduct of electronic surveillance, whether by use of wiretapping or microphones, and then only to obtain intelligence information necessary for the preservation of the national security. All electronic surveillance not in the national security field has been conducted in conformity with the court order procedures of the statute.

The procedures currently followed by the Department require that all requests for the authorization or re-authorization of a national security electronic surveillance are made by the Director of the Federal Bureau of Investigation to the Attorney General on behalf of the President of the United States. Each request is considered by the Attorney General in conjunction with all of the intelligence information, both foreign and domestic, available to the Executive Branch of the Government which bears upon the request. Up until the decision in the *Keith* case, it was necessary for the proposed surveillance to satisfy one or more of the following criteria:

(1) That it is necessary to protect the nation against actual or potential attack or any other hostile action of a foreign power.

(2) That it is necessary to obtain foreign intelligence information deemed essential to the security of the United States.

(3) That it is necessary to protect national security information against foreign intelligence activities.

(4) That it is necessary to protect the United States against the overthrow of the Government by force or other unlawful means.

(5) That it is necessary to protect the United States against a clear or present danger to the structure or the existence of its Government.

After the *Keith* decision, only the first three criteria (dealing with the foreign aspects of national security) have been taken into consideration. These criteria reflect the standards enunciated in 18 U.S.C. § 2511(3), enacted by the Omnibus Crime Control and Safe Streets Act of 1968. In those cases where a determination is made that one or more of the appropriate standards is met, a written authorization or a re-authorization for a specified period not to exceed three months is executed by the Attorney General.

APPENDIX A

THE WHITE HOUSE,
Washington, D.C., May 21, 1940.

Confidential.
Memorandum for: the Attorney General.

I have agreed with the broad purpose of the Supreme Court decision relating to *wire-tapping* in investigations. The Court is undoubtedly sound both in regard to the use of evidence secured over tapped wires in the prosecution of citizens in criminal cases; and is also right in its opinion that under ordinary and normal circumstances wire-tapping by Government agents should not be carried on for the excellent reason that it is almost bound to lead to abuse of civil rights.

However, I am convinced that the Supreme Court never intended any dictum in the particular case which it decided to apply to grave matters involving the defense of the nation.

It is, of course, well known that certain other nations have been engaged in the organization of propaganda of so-called "fifth columns" in other countries and in preparation for sabotage, as well as in actual sabotage.

It is too late to do anything about it after sabotage, assassinations and "fifth column" activities are completed.

You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigating agents that they are at liberty to secure information by listening devices direct to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies. You are requested furthermore to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens.

(s) F. D. R.

APPENDIX B

OCTOBER 9, 1941.

Confidential.
Memorandum for Mr. Hoover.

A good deal of my press conference yesterday was consumed in questions about wire tapping. I refused to comment on the Bridges incident, on the ground that it would be improper for me to comment on a case now pending before me.

I indicated that the stand of the Department would be, as indeed it had been for some time, to authorize wire tapping in espionage, sabotage and kidnapping cases, where the circumstances warranted. I described Section 605 of the Communications Act, pointing out that under the Statute interception alone was not illegal; that there must be both interception and divulgence or publication; that the Courts had held only that evidence could not be used which resulted from wire tapping; that the Courts had never defined what divulgence and publication was; that I would continue to construe the Act, until the Courts decided otherwise, not to prohibit interception of communications by an agent, and his reporting the result to his superior officer, as infraction of the law; that although this

could be said of all crimes, as a matter of policy wire tapping would be used sparingly, and under express authorization of the Attorney General.

This, I think, has clarified the situation.

I attach a brief memorandum opinion for me from the Assistant Solicitor General, supporting this construction of the Statute.

FRANCIS BIDDLE,
Attorney General.

OFFICE OF THE ATTORNEY GENERAL,
Washington, D.C., July 17, 1946.

The PRESIDENT,
The White House

MY DEAR MR. PRESIDENT: Under date of May 21, 1940, President Franklin D. Roosevelt, in a memorandum addressed to Attorney General Jackson, stated:

> "You are therefore authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigating agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies.

This directive was followed by Attorneys General Jackson and Biddle, and is being followed currently in this Department. I consider it appropriate, however, to bring the subject to your attention at this time.

It seems to me that in the present troubled period in international affairs, accompanied as it is by an increase in subversive activity here at home, it is as necessary as it was in 1940 to take the investigative measures referred to in President Roosevelt's memorandum. At the same time, the country is threatened by a very substantial increase in crime. While I am reluctant to suggest any use whatever of these special investigative measures in domestic cases, it seems to me imperative to use them in cases vitally affecting the domestic security, or where human life is in jeopardy.

As so modified, I believe the outstanding directive should be continued in force. If you concur in this policy, I should appreciate it if you would so indicate at the foot of this letter.

In my opinion, the measures proposed are within the authority of law, and I have in the files of the Department materials indicating to me that my two most recent predecessors as Attorney General would concur in this view.

Respectfully yours,

TOM C. CLARK,
Attorney General.

I concur, July 17, 1947.
HARRY S. TRUMAN.

APPENDIX D

CONFIDENTIAL

MARCH 16, 1955.

Mr. HOOVER.
HERBERT BROWNELL, Jr.,
Technical Surveillances.

I have your memorandum of March 8, 1955 on the above subject. In view of the fact that I personally explained to the President, the Cabinet, the National Security Council and the Senate and House Judiciary Committees during 1954 the present policy and procedure on wiretaps, at which time I referred specifically to the authorization letter to the Attorney General from President F. D. Roosevelt, I do not think it is necessary to re-open the matter at this time.

You will also remember I made several public speeches during 1954 on the legal basis for the Department of Justice policy and procedure on wiretaps.

CC—Mr. Rogers.
Mr. Tompkins with original of FBI memorandum referred to above.
Mr. Olney.

28

OFFICE OF THE ATTORNEY GENERAL,
Washington, D.C.

ORDER NO. 263–62: AMENDING ORDER NO. 3343

By virtue of the authority vested in me by Section 161 of the Revised Statutes (5 U.S.C. 22) and section 2 of Reorganization Plan No. 2 of 1950 (64 Stat. 1261), and in order to reflect the practice which has been in effect since May 21, 1940, the provision of the Manual of the Federal Bureau of Investigation, prescribed by and set forth in Order No. 3343 of March 15, 1940, is amended to read:

"Unethical Tactics: Entrapment or the use of any other improper, illegal, or unethical tactics in procuring information in connection with investigative activity will not be tolerated by the Bureau."

Existing instructions to the Federal Bureau of Investigation with respect to obtaining the approval of the Attorney General for wiretapping are continued in force.

ROBERT F. KENNEDY, *Attorney General.*

MARCH 13, 1963.

APPENDIX F

ADMINISTRATIVELY CONFIDENTIAL

THE WHITE HOUSE,
Washington, D.C., June 30, 1965.

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

The President is anxious that the attached memorandum which is designated "Administratively Confidential", be regarded as such that special efforts be made to respect the designation. For example, in compiling the information requested in the final paragraph, there is no reason to indicate this information has been requested by the President and a memorandum over your signature to operating personnel need not indicate this is a government-wide survey.

In relaying the basic guidelines set out in the President's memorandum this, too, can be a department or agency matter rather than directly attributed to the Presidential memorandum.

LEE C. WHITE,
Special Counsel to the President.

ADMINISTRATIVELY CONFIDENTIAL

THE WHITE HOUSE,
Washington, D.C., June 30, 1965.

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

I am strongly opposed to the interception of telephone conversations as a general investigative technique. I recognize that mechanical and electronic devices may sometimes be essential in protecting our national security. Nevertheless, it is clear that indiscriminate use of these investigative devices to overhear telephone conversations, without the knowledge or consent of any of the persons involved, could result in serious abuses and invasions of privacy. In my view, the invasion of privacy of communications is a highly offensive practice which should be engaged in only where the national security is at stake. To avoid any misunderstanding on this subject in the Federal Government, I am establishing the following basic guidelines to be followed by all government agencies:

(1) No federal personnel is to intercept telephone conversations within the United States by any mechanical or electronic device, without the consent of one of the parties involved, (except in connection with investigations related to the national security.)

(2) No interception shall be undertaken or continued without first obtaining the approval of the Attorney General.

(3) All federal agencies shall immediately conform their practices and procedures to the provisions of this order.

Utilization of mechanical or electronic devices to overhear non-telephone conversations is an even more difficult problem, which raises substantial and unresolved questions of Constitutional interpretation. I desire that each agency conducting such investigations consult with the Attorney General to ascertain whether the agency's practices are fully in accord with the law and with a decent regard for the rights of others.

Every agency head shall submit to the Attorney General within 30 days a complete inventory of all mechanical and electronic equipment and devices used for or capable of intercepting telephone conversations. In addition, such reports shall contain a list of any interceptions currently authorized and the reasons for them.

LYNDON B. JOHNSON.

APPENDIX G

FEBRUARY 26, 1952.

MR. HOOVER.
Director, Federal Bureau of Investigation,

ATTORNEY GENERAL
Wire Tapping Surveillances
Personal and confidential

Reference is made to your memoranda relative to wire tapping surveillances.

There is pending, as you know, before the Congress legislation that I have recommended which would permit wire tapping under appropriate safeguards and make evidence thus obtained admissible. As you state, the use of wire tapping is indispensible in intelligence coverage of matters relating to espionage, sabotage, and related security fields. Consequently, I do not intend to alter the existing policy that wire tapping surveillance should be used under the present highly restrictive basis and when specifically authorized by me.

The use of microphone surveillance which does not involve a trespass would seem to be permissible under the present state of the law, *United States* v. *Goldstein*, 316 U.S. 1. Such surveillances as involve trespass are in the area of the Fourth Amendment, and evidence so obtained and from leads so obtained is inadmissible.

The records do not indicate that this question dealing with microphones has ever been presented before; therefore, please be advised that I cannot authorize the installation of a microphone *involving a trespass* under existing law.

It is requested when any case is referred to the Department in which telephone, microphone or other technical surveillances have been employed by the Bureau or other Federal Agencies (when known) that the Department be advised of the facts at the time the matter is first submitted.

Previous interpretations which have been furnished to you as to what may constitute trespass in the installation of microphones, suggest that the views expressed have been tentative in nature and have attempted to predict the course which courts would follow rather than reflect the present state of the law. It is realized that not infrequently the question of trespass arises in connection with the installation of a microphone. The question of whether a trespass is actually involved and the second question of the effect of such a trespass upon the admissibility in court of the evidence thus obtained, must necessarily be resolved according to the circumstances of each case. The Department in resolving the problems which may arise in connection with the use of microphone surveillance will review the circumstances in each case in the light of the practical necessities of investigation and of the national interest which must be protected. It is my opinion that the Department should adopt that interpretation which will permit microphone coverage by the FBI in a manner most conducive to our national interest. I recognize that for the FBI to fulfill its important intelligence function, considerations of internal security and the national safety are paramount and, therefore, may compel the unrestricted use of this technique in the national interest.

30

APPENDIX H

Confidential

Director, Federal Bureau of Investigation.

The Attorney General.

MICROPHONE SURVEILLANCE

The recent decision of the Supreme Court entitled *Irving* v. *California*, 347 U.S. 128, denouncing the use of microphone surveillances by city police in a gambling case makes appropriate a reappraisal of the use which may be made in the future by the Federal Bureau of Investigation of microphone surveillance in connection with matters relating to the internal security of the country.

It is clear that in some instances the use of microphone surveillance is the only possible way of uncovering the activities of espionage agents, possible saboteurs, and subversive persons. In such instances I am of the opinion that the national interest requires that microphone surveillance be utilized by the Federal Bureau of Investigation. This use need not be limited to the development of evidence for prosecution. The FBI has an intelligence function in connection with internal security matters equally as important as the duty of developing evidence for presentation to the courts and the national security requires that the FBI be able to use microphone surveillance for the proper discharge of both of such functions. The Department of Justice approves the use of microphone surveillance by the FBI under these circumstances and for these purposes.

I do not consider that the decision of the Supreme Court in *Irving* v. *California*, *supra*, requires a different course. That case is readily distinguishable on its facts. The language of the Court, however, indicates certain uses of microphones which it would be well to avoid, if possible, even in internal security investigations. It is quite clear that in the *Irving* case the Justices of the Supreme Court were outraged by what they regarded as the indecency of installing a microphone in a bedroom. They denounced the utilization of such methods of investigation in a gambling case as shocking. The Court's action is a clear indication of the need for discretion and intelligent restraint in the use of microphones by the FBI in all cases, including internal security matters. Obviously, the installation of a microphone in a bedroom or in some comparable intimate location should be avoided wherever possible. It may appear, however, that important intelligence or evidence relating to matters connected with the national security can only be obtained by the installation of a microphone in such a location. It is my opinion that under such circumstances the installation is proper and is not prohibited by the Supreme Court's decision in the *Irving* case.

Previous interpretations which have been furnished to you as to what may constitute trespass in the installation of microphones, suggest that the views expressed have been tentative in nature and have attempted to predict the course which courts would follow rather than reflect the present state of the law. It is realized that not infrequently the question of trespass arises in connection with the installation of a microphone. The question of whether a trespass is actually involved and the second question of the effect of such a trespass upon the admissibility in court of the evidence thus obtained, must necessarily be resolved according to the circumstances of each case. The Department in resolving the problems which may arise in connection with the use of microphone surveillance will review the circumstances in each case in the light of the practical necessities of investigation and of the national interest which must be protected. It is my opinion that the Department should adopt that interpretation which will permit microphone coverage by the FBI in a manner most conducive to our national interest. I recognize that for the FBI to fulfill its important intelligence function, considerations of internal security and the national safety are paramount and, therefore, may compel the unrestricted use of this technique in the national interest.

31

APPENDIX I

MAY 4, 1961.

To: Mr. Byron R. White, Deputy Attorney General.
From: Director, FBI.
Subject: Technical and microphone surveillances.

In connection with the Attorney General's contemplated appearance before the Senate Subcommittee on Constitutional Rights, our views on the use of microphone surveillances in FBI cases are set forth for your consideration. Under date of April 21, 1961, we furnished our comments on S. 1495, which is proposed legislation on wire tapping.

Our policy on the use of microphone surveillances is based upon a memorandum from former Attorney General Herbert Brownell dated May 20, 1954, in which he approved the use of microphone surveillances with or without trespass. In this memorandum Mr. Brownell said in part:

"I recognize that for the FBI to fulfill its important intelligence function, considerations of internal security and the national safety are paramount and, therefore, may compel the unrestricted use of this technique in the national interest."

In light of this policy, in the internal security field, we are utilizing microphone surveillances on a restricted basis even though trespass is necessary to assist in uncovering the activities of Soviet intelligence agents and Communist Party leaders. In the interests of national safety, microphone surveillances are also utilized on a restricted basis, even though trespass is necessary, in uncovering major criminal activities. We are using such coverage in connection with our investigations of the clandestine activities of top hoodlums and organized crime. From an intelligence stand-point, this investigative techniques has produced results unobtainable through other means. The information so obtained is treated in the same manner as information obtained from wire taps, that is, not from the standpoint of evidentiary value but for intelligence purposes.

There is no Federal legislation at the present time pertaining to the use of microphone surveillances. The passage of any restrictive legislation in this field would be a definite loss to our investigative operations, both in the internal security field and in our fight against the criminal element. This is especially true in the case of organized crime where we have too few weapons at our command to give up the valuable technique of microphones.

[Memorandum from Elliot Richardson to Clarence Kelley, with covering memorandum from Robert G. Dixon to Elliot Richardson.]

MEMORANDUM FOR THE ATTORNEY GENERAL

SEPTEMBER 6, 1973.

Re: FBI proposed executive order on domestic surveillance.

Attached is a reply for your signature to a memorandum from the Director of the FBI proposing an Executive order concerning FBI domestic Surveillance authority.

Mr. Ruckelshaus has approved the memorandum.

ROBERT G. DIXON, Jr.,
Assistant Attorney General,
Office of Legal Council.

MEMORANDUM FOR THE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

SEPTEMBER 12, 1973.

Re: Proposed executive order concerning scope of FBI jurisdiction in domestic intelligence investigations.

I have your memorandum of August 7, 1973, which recommends the issuance of an Executive order concerning the authority of the FBI to conduct domestic intelligence operations. Your memorandum indicates that the proposed order is

designed to accomplish several objectives (1) to establish that the FBI has been instructed to engage in domestic intelligence operations; (2) to supplement the statutory authority of the FBI by delegating any constitutional power the President may have in this area; and (3) to direct the Attorney General to establish guidelines for domestic intelligence.

It is possible that an Executive order or other directive on this subject may serve a useful purpose. The President may have some power in this area under the Constitution which is broader than that found in present statutes or in existing presidential directives. In the *Keith* case (407 U.S. 297), for example, the Court recognized "that the President of the United States has the fundamental duty, under Art. II, § 1, of the Constitution, to 'preserve, protect and defend the Constitution of the United States.' Implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means." 407 U.S. at 310. See also 407 U.S. at 312, 322. It is arguable that in some cases this power may be beyond that given to the Attorney General under 28 U.S.C. § 533 and other statutes or which has previously been delegated by the Attorney General to the FBI. 28 CFR § 0.85.[1]

Similarly, there may be occasion to establish with some degree of visibility that the FBI is being given policy direction in the domestic surveillance area by both the President and the Attorney General.

I believe, however, that it would be premature to recommend to the President that an Executive order be issued until we were fairly certain in our own minds as to how much should be and can be accomplished at each level of delegation. If we are to have the President direct the issuance of guidelines we should first have a clear idea of whether it is feasible to publish such guidelines and what their content should be.

As you know, I have asked Mr. Ruckelshaus to consult with you on a variety of matters relating to intelligence questions. It would be desirable to consider the necessity of an Executive order as a part of the agenda which you are to review with him.

ATTORNEY GENERAL.

OFFICE OF THE ATTORNEY GENERAL,
Washington, D.C., September 12, 1973.

Hon. J. W. FULBRIGHT,
Chairman, Senate Foreign Relations Committee,
Washington, D.C.

DEAR MR. CHAIRMAN: During the confirmation hearings of Dr. Kissinger, a question was raised as to this Administration's position concerning the power of the Executive to conduct electronic surveillance without warrant in the national security field. Dr. Kissinger said that he would try to elicit a statement for the record that would clarify our general policy on this matter.

I believe that there will continue to be situations which jusify the conduct of electronic surveillance for the purposes of national security. This surveillance is carried out to meet the obligations of the President as both Commander-in-Chief and as the Nation's instrument for foreign affairs. I will continue to attempt to ensure that a genuine national security interest is, in fact involved whenever we invoke this power and that we operate within the limits set by Congress and the courts.

The Department of Justice scrupulously observes the law as interpreted by the courts. There may be questions as to what certain decisions mean and whether surveillance, such as that discussed by the committee, has been affected by later court decision. These and other issues are before the courts now and we expect any ambiguities to be settled within the normal judicial process. The policy statement that follows therefore refers to procedures for any surveillance that may be carried out at present.

A year ago in the *Keith* case (407 U.S. 297), the Supreme Court ruled unanimously that the Government may not carry on electronic surveillance in domestic security operations, as opposed to foreign intelligence operations, without first obtaining a judicial warrant. The Court pointed out that it was condemning warrantless electronic surveillance carried out in *domestic* security cases directed at a "domestic organization (whether formally or informally constituted) com-

[1] In speculating on this point I do not, of course, intend to authorize any action by the Bureau or to suggest that the limits on electronic surveillance set out in the *Keith* case should not be closely followed.

posed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies." The *Keith* decision necessarily is Departmental policy and is being followed.

Although the *Keith* case did not address warrantless *national* security electronic surveillance, to date, the lower courts which have addressed the problem have agreed with the contention of this Department that a judicial warrant is not a necessary requirement for the Government's use of electronic surveillance to obtain foreign intelligence or foreign policy information necessary for the protection of national security. *E.g., United States* v. *Clay*, 430 F. 2d 165 (5th Cir. 1970), *reversed on other grounds*, 403 U.S. 698 (1971); *United States* v. *Brown*, 317 F. Supp. 531 (E.D. La., 1970) *affirmed*, No. 72-2181 (5th Cir., Aug. 22, 1973); *United States* v. *Smith*, 321 F. Supp. 424 (C.D. Calif. 1971); *Zweibon* v. *Mitchell*, 42 U.S. L. Week 2054 (1973). Pending a decision on this issue by the Supreme Court, I believe that we are justified in relying on the case law as it is being developed in the lower courts to conduct national security electronic surveillance, without warrant, in a limited number of cautiously and meticulously reviewed instances.

When Congress enacted legislation in 1968 requiring a judicial warrant for the use of electronic surveillance in investigations of violations of certain criminal laws, it made clear that it did not intend to add or subtract from whatever measure of constitutional power the President may have to use electronic surveillance in the national security field. However, as a guide, it set forth a number of purposes, divided between the domestic and foreign aspects of national security, that it understood to be proper for the exercise of Presidential power. The *Keith* decision subsequently held that this power could not, in the absence of a warrant, be exercised for the *domestic* security purposes mentioned by Congress. However, as a matter of policy, I shall keep in mind the contours of the President's power suggested by Congress in the 1968 law as it relates to foreign intelligence. In general, before I approve any new application for surveillance without a warrant, I must be convinced that it is necessary (1) to protect the nation against actual or potential attack or other hostile acts of a foreign power; (2) to obtain foreign intelligence information deemed essential to the security of the United States; or (3) to protect national security information against foreign intelligence activities. 18 U.S.C. 2511(3).

As the Supreme Court itself observed in *Keith*, it may well be difficult to distinguish between "domestic" and "foreign" unlawful activities directed against the United States where there are relationships in varying degrees between domestic groups or organizations and foreign powers, or their agents. All I can say is that, as the applications are presented to me, I will, together with my staff, try scrupulously to follow the guidance and instruction given to us by Congress and the courts, bearing in mind the importance of balancing individual privacy with the needs of national security.

In addition, there is ongoing in the Department a full-scale effort under my and Bill Ruckelshaus' immediate supervision, to derive new standards and guidelines for use of electronic surveillance in both domestic criminal matters, as well as for national security purposes. It is our hope that we will be able to give these standards precise public articulation and thus foster better understanding of the scope and nature of our limited use of electronic surveillance. Also, as I mentioned the other day, the new FBI Oversight Subcommittee of the Senate Judiciary Committee will allow the Congress to be better informed about these activities.

With kindest regards,

Sincerely,

ELLIOT L. RICHARDSON,
Attorney General.

[Memorandum from Robert G. Dixon, Jr., to Elliot L. Richardson]

MEMORANDUM FOR THE ATTORNEY GENERAL

JUNE 26, 1973.

Re: National security electronic surveillances.

This is in response to a memorandum from your office asking for an analysis of the state of the law regarding national security electronic surveillance. This memorandum will discuss (I) whether the Government presently has the power under the Constitution to engage in electronic surveillance without

a warrant; (II) the scope of that power, and (III) what legal alternatives may be available.

I.

A year ago in the *Keith* case,[1] the Supreme Court ruled unanimously that electronic surveillance in domestic as opposed to foreign intelligence matters could not be accomplished without a warrant.[2]

The Court held that (1) the Omnibus Crime Control and Safe Streets Act (18 U.S.C. § 2511(3)) did not give the Executive authority to conduct warrantless national security electronic surveillances but merely disclaimed any intent to interfere with that power to the extent that it might exist,[3] and (2) the Fourth Amendment (which shields private speech from unreasonable surveillance) requires prior judicial approval for domestic security surveillance.

The Court also said in *Keith* that "the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers within or without this country." 407 U.S. at 308; see also 321–22. The question arises therefore as to what view this Department should take of the law in light of this disclaimer.

In this connection the following should be noted:

(1) There is a fairly substantial body of opinion in the lower courts upholding, without exception, the power of the Government to engage in electronic surveillance in foreign intelligence cases without a warrant. In the absence of a definitive ruling by the Supreme Court it seems that, as a legal matter, the Department can point to these opinions as justifying continued warrantless surveillance of this kind. These opinions are *United States* v. *Clay a/k/a Ali* (S.D. Tex. 1969, Cr. No. 67–H–94, unreported), *affirmed*, 430 F. 2d 165 (5th Cir. 1970), *reversed on other grounds* 403 U.S. 698 (1971); *United States* v. *Butenko*, 318 F. Supp. 66 (D.N.J. 1970), *appeal pending* (3d Cir., No. 72–1741); *United States* v. *Smith*, 321 F. Supp. 424 (C.D. Calif. 1971) (dictum); *United States* v. *Brown*, 317 F. Supp. 531, 536 (E.D. La. 1970); *United States* v. *O'Baugh*, 304 F. Supp. 767 (D.D.C. 1969); *United States* v. *Stone*, 305 F. Supp. 75 (D.D.C. 1969); *United States* v. *Dellinger*, (N.D. Ill. 1970, No. 69 CR 180, unreported); *United States* v. *Enten*, (D.D.C., 1971, Crim. No. 166–71, unreported) *appeal pending* (D.C. Cir. No. 71–1774); *United States* v. *Hoffman*, (D.D.C., 1971, Criminal No. 973–71, unreported).

In general, these cases rely either explicitly or implicitly on the view that the surveillances are authorized by the constitutional power of the President as Commander-in-Chief and as the Nation's organ for foreign affairs and that the courts are not equipped to decide what is and what is not a threat to national security. *Cf. Chicago & Southern Airlines* v. *Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948)

(2) There may be an opportunity for the Supreme Court to rule on this matter at some time in the future. There are two cases which have been briefed and argued and await decision in the appellate courts, one in the Third Circuit and one in the U.S. Court of Appeals for the District of Columbia, both of which present the foreign intelligence issue squarely (*United States* v. *Butenko and Ivanov*, No. 72–1741, 3rd Cir.; *United States* v. *Enten*, No. 71–1774, D.C. Cir.). There is, of course, no assurance that the Supreme Court will take the opportunity, should it arise. As in *Keith*, the Supreme Court in the past has avoided opportunities to rule on the issue. After the Fifth Circuit ruled in the Clay case in 1970 that electronic surveillance for foreign intelligence purposes was lawful

---

[1] *United States* v. *United States District Court for the Eastern District of Michigan*, 407 U.S. 297 (1972). *Keith* was the District Judge in the case who was the subject of a petition for a writ of mandamus by the Government after he ruled that the surveillance carried out was unlawful.

[2] Immediately thereafter, Attorney General Kleindienst announced that in accordance with that decision the Department would terminate all electronic surveillance in cases involving domestic security that conflict with the *Keith* case. (Statement of June 19, 1972.)

[3] "Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power."

(*United States* v. *Clay*, *supra*) certiorari was granted on issues other than surveillance and the decision below was reversed by the Court on other grounds. In *United States* v. *Katz*, 389 U.S. 347 (1967), the Court held that electronic surveillance was covered by the Fourth Amendment but, at the same time, specifically noted that it was not ruling on situations involving national security. 389 U.S. at 358, note 23.

(3) There are indications that the Supreme Court at best will be divided on the issue and it is possible that a majority might rule against the Department. Three Justices now sitting appear to have already expressed their views on this issue. In *Katz*, *supra*, where electronic eavesdropping was held covered by the Fourth Amendment, Justices Douglas and Brennan stated forcefully in a concurring opinion that the Fourth Amendment prohibited national security surveillance without a warrant (389 U.S. at 359), while Justice White, in a separate concurrence took the opposite view (389 U.S. at 362).

The Douglas-Brennan opinion stated:

> Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be. Under the separation of powers created by the Constitution, the Executive Branch is not supposed to be neutral and disinterested. Rather it should vigorously investigate and prevent breaches of national security and prosecute those who violate the pertinent federal laws. The President and Attorney General are properly interested parties, cast in the role of adversary, in national security cases. They may even be the intended victims of subversive action. Since spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers like petitioner, I cannot agree that where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate. (389 U.S. at 359).

Clearly, the argument that electronic surveillance without warrant is necessary for counter-intelligence or similar matters is not going to sit well with these two members of the Court.

Moreover, the reasoning in the *Keith* case itself suggests that the Court may not be readily persuaded of the Government's case. Although it is true that the Court specifically reserved the foreign intelligence issue, at no point did it volunteer any reasons as to why, as a mater of constitutional law it might be willing to make this distinction when presented with a proper case. To the contrary, the reasoning in *Keith* seems to anticipate and reject arguments the Department is making at this time in the "foreign intelligence" cases in the lower courts. Thus, in the case pending in the Third Circuit the Department has presented the following arguments why judicial approval should not be required for foreign intelligence surveillance (Brief for Appellee, *United States* v. *Butenko and Ivanov*, Docket No. 72–1741, pp. 34–34.):

(a) Information on which such surveillance is based is highly confidential and must be kept secret.

(b) Sensitive information is "simply not susceptible of evaluation by persons who do not regularly deal with foreign affairs matters."

(c) In foreign intelligence surveillances, "the justification * * * cannot be simply stated or easily demonstrated;" it requires the drawing of subtle inferences. Almost without exception there is no known criminal activity involved as such.

The opinion in *Keith* appears to respond to the listed arguments with the following:

(a) As to secrecy: "The investigation of criminal activity has long involved imparting sensitive information to judicial officers who have respected the confidentialities involved. Judges may be counted upon to be especially conscious of security requirements in national security cases. [The 1968 electronic surveillance statute] already has imposed this responsibility on the judiciary in connection with such crimes as espionage, sabotage, and treason * * *, each of which may involve domestic as well as foreign security threats. Moreover, a warrant application involves no public or adversary proceedings: it is an *ex parte* request * * *. Whatever security dangers clerical and secretarial personnel may pose can be minimized by proper administrative procedures, possibly to the point of allowing the Government itself to provide the necessary clerical assistance." 407 U.S. at 320–21.

(b) As to complexity and the need for sophistication: "We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. * * * security surveillance involves different considerations from the surveillance of 'ordinary crime.'" 407 U.S. at 320.

The Court also suggested that in "sensitive cases," authorizations might be made by a designated court, such as the Court of Appeals for the District of Columbia. 407 U.S. at 323. Although the Court did not explicitly say so, one implication is that if all foreign intelligence applications were made to the same court, it might be more difficult for the Government to argue that the court lacked the necessary background to understand them.

(c) As to the difficulty of justification and the absence of conventional criminal activity, the Court said: "Different standards may be compatible with the Fourth Amendment if they were reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection." 407 U.S. at 322–23. In support, the Court cited its recent decision holding that a health official need not show the same kind of proof to a magistrate to obtain a warrant as one who would search for the fruits of crime. *Camara* v. *Municipal Court*, 387 U.S. 523 (1967).

The Court made the following additional points in *Keith* which suggest that it may not readily recognize an exception to the warrant clause of the Fourth Amendment even for foreign intelligence:

(a) The use of electronic surveillance is not a welcome development "even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens." (407 U.S. at 312).

(b) "Though physical entry of the home is the chief evil against which the * * * Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance. * * * [B]road and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate Fourth Amendment safeguards." (407 U.S. 313.)

(c) "National security cases * * * often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech." (407 U.S. 313.)

(d) "Inherent in the concept of a warrant is its issuance by a 'neutral and detached magistrate.' * * * The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." 407 U.S. at 316–17.

As we noted earlier, we believe that the Department is justified in continuing to rely on the clear weight of the case law until the Supreme Court rules otherwise. However, close analysis of *Katz* and *Keith* suggests that the ultimate decision of the Court may be against the position the Department is now arguing.

II.

The next question which arises relates to defining the scope of surveillance that may still be carried on without a warrant after *Keith*.

At the outset, we note that the Omnibus Crime Control and Safe Streets Act of 1968 merged procedures for obtaining warrants for wiretapping and microphone surveillance or bugging. 18 U.S.C. 2510. The statement of facts in *Keith* shows that wiretapping was there involved. 407 U.S. at 300. However, the Court uses the generic term "electronic surveillance" throughout its opinion. The Court has also indicated that it sees no distinction in constitutional principle between the two (*cf. Katz* v. *United States*, 389 U.S. 347 (1967)), and we therefore use the term "electronic surveillance" here to include both wiretapping and bugging.

The 1968 Act stated that Congress did not intend to interfere with the constitutional power of the President. 18 U.S.C. 2511(3). The Act purported to describe the possible outlines of that power in the light of the criteria set out below, leaving it to the courts to resolve the issues involved. See *Keith* at 407 U.S. 301–308. As noted, *Keith* held that 18 U.S.C. 2511(3) is not in itself a grant of authority to conduct warrantless national security surveillances and that there is no power to conduct such surveillance in domestic security situations.

We are thus left with the "foreign security" criteria in 18 U.S.C. 2511(3), which have not been discussed by the Supreme Court and which relate to presidential power necessary: (1) to protect the nation against actual or potential attack or other hostile acts of a foreign power; (2) to obtain foreign intelligence information deemed essential to the security of the United States; or (3) to protect national security information against foreign intelligence activities. 18 U.S.C. 2511(3).

The Court said these criteria, as they appear in § 2511(3), are an expression of neutrality rather than a measure of executive authority. 407 U.S. at 308. However, they are not totally neutral since they can be read as setting outer limits on possible constitutional power in this area. Section 2511(3) is, in effect, an exception from prohibitions in the 1968 Act and the Communications Act. Failure to bring surveillances within the rubric of § 2511(3) would seem to make them illegal *per se* under the general prohibitions relating to electronic surveillance found in 18 U.S.C. 2510–20. See White, J., concurring in *Keith* (407 U.S. at 335).

Keith itself provides other limits which relate more to the nature of the subjects of surveillance rather than to ultimate purpose (which is the focus of 18 U.S.C. 2511(3)). Thus the Court made clear that the surveillance power described may not be used against "domestic organizations" which have "no significant connection with a foreign power, its agents or agencies." 407 U.S. at 309, note 8. The lower court decisions, which are all pre-*Keith*, do not make any further distinctions along this line. This Department has publicly placed the following gloss on these words:

"We do not interpret this as meaning casual, unrelated contacts and communications with foreign governments or agencies thereof. We would not try to apply this standard without the presence of such factors as substantial financing, control by or active collaboration with a foreign government and agencies thereof in unlawful activities directed against the Government of the United States."

(Statement by Kevin Maroney, Deputy Assistant Attorney General, Internal Security Division, on Electronic Surveillance before Senate Subcommittee on Administrative Practice and Procedure, June 29, 1972). Presumably, this means that before electronic surveillance power is used against groups composed of citizens a rather clear showing of possible law violation must be shown. When dealing with purely foreign entities, the only limits, as of now, are those found in § 2511(3).

III.

The Department now has a number of alternatives which it may follow:

(1) It can continue the existing policy of engaging in electronic surveillance for foreign intelligence purposes without a warrant. The difficulty with this posture is its uncertainty. Before a final decision is made by the Supreme Court, there may be several years of remands and hearings to determine whether electronic surveillance is foreign or domestic within the meaning of *Keith*. This may be time consuming and, since illegal taps and bugs must be disclosed (*Alderman* v. *United States*, 394 U.S. 165 (1969)), embarrassing. Even if the Supreme Court does ultimately hold that there are exceptions to the Fourth Amendment for foreign intelligence surveillance there is no assurance that the warrant exception will be as wide in scope as what is suggested by 18 U.S.C. 2511(3).

If the Government loses in the Supreme Court, the fall-out may be extensive since each tap or bug is capable of picking up hundreds of subjects. As past cases demonstrate, there is no such thing as a "purely foreign" tap since citizens who later become involved as defendants are also picked up. See *e.g.*, *United States* v. *Clay*, *supra*. The recent Watergate hearings have even revealed an instance of a defendant deliberately making calls to embassies whose lines he believed tapped in order to complicate matters for the prosecution.

One of the arguments raised against obtaining warrants is the possibility that there will be security leaks. However, it can be argued that as long as the legality of this surveillance remains in a gray area, the necessary hearings and inspections (both *in camera* and in open court) and the proliferation of private suits will actually produce more leaks and more publicity than any system for obtaining warrants.

(2) There are a number of possibilities for obtaining warrants for surveillance for foreign intelligence purposes.

(a) Title III of the Omnibus Crime Control and Safe Streets Act now authorizes warrants for such crimes as espionage, sabotage, and treason. 18 U.S.C. 2516(1)(a) and (c). It may be that there are cases where a warrant could be

obtained under Title III but where warrantless surveillance is now used instead. In applications to the Attorney General for warrantless surveillance perhaps an explanation should be included as to why Title III is not being used.

(b) It is possible that without new legislation the courts will grant warrants for electronic surveillance under standards less onerous than Title III. In *Osborn* v. *United States*, 385 U.S. 323, 328–311 (1966), judicial approval was obtained for electronic surveillance even though no statute or rule authorized such a procedure at the time. Similarly, following *Camara*, *supra*, 387 U.S. 523, which held that warrants were necessary for administrative inspections, the Bureau of Narcotics and Dangerous Drugs succeeded in getting some courts to issue administrative warrants although legislation authorizing them had not yet been enacted. The *Keith* (407 U.S. at 322–23) and *Camara* (387 U.S. at 534–35) cases seem to indicate that the Court would rather make the warrant requirement flexible than create exceptions to it. Mr. Maroney's statement of June 29, 1972, (quoted in Part II) indicates that, at least in cases involving United States citizens or groups, there must be evidence of "unlawful activities directed against the Government of the United States." Therefore, it may well be possible to demonstrate to a court something akin to conventional notions of probable cause when requesting warrants in this type of case.

(c) Another possibility is legislation specifically authorizing the kind of procedure contemplated under (b). In *Keith* the Court suggested that procedures with standards different from those in Title III could be enacted for domestic intelligence purposes. (407 U.S. at 322.) Presumably, the same reasoning would support legislation with standards that are less rigorous than Title III in the foreign intelligence field.

Since our Office has never seen the applications for electronic surveillance submitted to the Attorney General and since we have no specific knowledge of cases now pending and the problems they present, we cannot make any firm recommendation as to how the Department should proceed. We suggest only that a risk-benefit analysis based on a hard appraisal of the legal situation may well prove useful to the Department in the long run.

ROBERT G. DIXON, JR.,
Assistant Attorney General,
Office of Legal Counsel.

[Followup memo from Robert G. Dixon, Jr., to Elliot L. Richardson]

MEMORANDUM FOR THE ATTORNEY GENERAL

JULY 5, 1973.

Re: National security electronic surveillances.

On June 26, 1973, we sent you an analysis of the state of the law regarding national security electronic surveillance. Our memorandum noted (p. 3) a case under advisement in the Third Circuit presenting the issue whether the Executive has the power under the Constitution to engage in electronic surveillance for foreign intelligence purposes without a warrant, and to use the evidence thus obtained in a criminal prosecution. That case has now been decided. *United States* v. *Butenko and Ivanov* (No. 72–1741, 3rd Cir., June 21, 1973).

The court did not, however, reach the key constitutional question left undecided in *United States* v. *U.S Dist. Ct.*, 407 U.S. 297 (1972).

The majority in *Butenko* held that the use in a criminal case of evidence obtained through electronic surveillance (wire tapping) conducted in 1963 violated the Communications Act of 1934, 47 U.S.C. 605, which makes it unlawful to intercept *and* divulge wire communications.

The Omnibus Crime Control and Safe Streets Act of 1968 was not interpreted since the governing statute was § 605; the 1968 Act has a specific exemption from the Communications Act for national security electronic surveillance. 18 U.S.C 2511(3). The court assumed, for the sake of argument, that in 1963 the President had a constitutional power to conduct a surveillance of foreign agents, but concluded that Congress also had the power to forbid disclosure under the Communications Act in a criminal prosecution.

A dissenting opinion held (1) that the Communications Act was not intended to prohibit the President, or those acting on his behalf, from intercepting telephone communications and making use of the material in cases involving the gathering of foreign intelligence information, and (2) that the President had the power under the Constitution to conduct "reasonable" electronic surveillance

without a warrant and that the use of the evidence thus obtained did not violate the Fourth Amendment.

There is nothing in the opinion inconsistent with the view that the President may have the power to conduct foreign intelligence electronic surveillance without a warrant after 1968 and use the resulting evidence. However, the decision is significant in that it holds that the power is subject to regulation by Congress, and that the area remains a source of difficulty.

No decision has yet been made in the Department as to whether to petition for a rehearing *en banc* or to petition the Supreme Court for certiorari.

ROBERT G. DIXON, Jr.,
Assistant Attorney General,
Office of Legal Counsel.

U.S. Department of Justice, Standards and procedures for reviewing requests for electronic surveillance. Attorney General Edward Levi. Letter to Senator Edward M. Kennedy expressing support of "The Foreign Intelligence Surveillance Act of 1976" (S. 3197), June 29, 1975. Source: U.S. Congress. Senate. Committee on the Judiciary. Foreign Intelligence Surveillance Act of 1976. Report (to accompany S. 3197). July 15, 1976. Senate Report no. 94–1035.

LETTER

Under the standards and procedures established by the President, the personal approval of the Attorney General is required before any nonconsensual electronic surveillance may be instituted within the United States without a judicial warrant. All requests for surveillance must be made in writing by the Director of the Federal Bureau of Investigation and must set forth the relevant factual circumstances that justify the proposed surveillance. Both the agency and the Presidential appointee initiating the request must be identified. Requests from the Director are examined by a special review group which I have established within the Office of the Attorney General. Authorization will not be granted unless the Attorney General has satisfied himself that the requested electronic surveillance is necessary for national security or foreign intelligence purpose important to national security.

In addition, the Attorney General must be satisfied that the subject of the surveillance is either assisting a foreign power or foreign-based political group, or plans unlawful activity directed against a foreign power or foreign-based political group. Finally, he must be satisfied that the minimum physical intrusion necessary to obtain the information will be used.

All authorizations are for a period of ninety days or less, and the specific approval of the Attorney General is again required for continuation of the surveillance beyond that period. The Attorney General has also been directed to review all electronic surveillance on a regular basis to ensure that the aforementioned criteria are satisfied. Pursuant to the mandate of *United States* v. *United States District Court*, electronic surveillance without a judicial warrant is not conducted where there is no foreign involvement.

U.S. Federal Communications Commission. Memorandum on the use of telephone extension to monitor improper communications; Administrative Order no. 12; and letter from Dean Burch, Chairman, FCC, to John Moss, Chairman, House Committee on Government Operations. U.S. Congress. House. Committee on Interstate and Foreign Commerce. Special Subcommittee on Investigations. FCC monitoring of employees' telephones. Hearings, 92d Congress, 2d session. March 28 and May 16, 1972. pp. 48-52.

EXHIBIT D

MEMORANDUM ON THE USE OF TELEPHONE EXTENSION TO MONITOR IMPROPER COMMUNICATIONS

INTRODUCTION

The purpose of this memorandum is to explore the legality of Commission monitoring of its own telephone lines in order to uncover suspected improper communications. I am specifically concerned with the following fact situation: (1) at one time during 1970 it was suspected that documents intended for Commission use only were regularly being disclosed to outside parties, (2) the evidence indicated that these disclosures were being made through the use of a Commission telephone after the close of normal working hours, and (3) the evidence further indicated that the telephone disclosures were being made by a former FCC employee who was being illegally aided by an employee of the Commission. On the basis of this information, it was decided that a telephone extension should be installed in another room so as to permit Commission security personnel to monitor the illicit calls.

The law applicable to surveillance activities of this type is contained in the Omnibus Crime Control and Safe Streets Act of 1968, and in the Fourth Amendment to the U.S. Constitution.

A. The Omnibus Crime Control and Safe Streets Act of 1968

The Omnibus Crime Control and Safe Streets Act of 1968 makes illegal the conduct of any person who willfully intercepts wire or oral communications by means of an "electronic, mechanical, or other device." 18 U.S.C. § 2511(1)(a). This Act supersedes Section 605 of the Communications Act of 1934, 47 U.S.C. § 605, which until 1968 provided that "no person not being authorized by the sender shall intercept any communication and divulge or publish the . . . substance . . . of such intercepted communication to any person . . ." With the 1968 adoption of the Omnibus Crime Act, this Section of the Communications Act was amended to apply only to the interception and divulgence of *radio* communications. The interception and divulgence of wire communications is no longer prohibited by the Communications Act. The Omnibus Crime Act, however, makes interceptions of wire communications themselves illegal, whether or not they are followed by a divulgence.

In considering the legality of the Commission's monitoring activity, it should be kept firmly in mind that the line under surveillance was being used by a non-employee, after normal working hours, and without proper authorization. Both common sense and official regulations make it plain that government telephones are provided for official use only. In the late 1960's G.S.A. notices specifically informed FCC employees that "GOVERNMENT TELEPHONES ARE PROVIDED FOR OFFICIAL USE ONLY AND ARE NOT TO BE USED FOR RECEIVING OR MAKING PERSONAL CALLS." G.S.A. Notice DC 69-3770, September 19, 1968. In the circumstances of this case it is plain that the non-employee who was using the Commission's phones was doing so without proper authority. Indeed, when questioned about the matter, the individual admitted having used the lines for "personal" calls.

The cases decided under old Section 605 of the Communications Act generally upheld surveillance where communications facilities were being utilized by per-

[1] Public Law 89-478, effective July 4, 1967.

sons who had no authority to use them. The courts considered persons illegally using communications facilities to be "trespassers" who had no right of privacy in the use of such facilities. In *United States* v. *Sugden*, 226 F. 2d 281 (9th Cir. 1955), aff'd *Per Curiam* 351 U.S. 916 (1956), a trespasser theory was applied in upholding the monitoring of broadcasts by unlicensed radio operators. In *Brandon* v. *United States*, 382 F. 2d 607 (10th Cir. 1967), it was held that Section 605 did not prohibit the telephone company from monitoring long-distance calls which were made with the aid of a device which illegally by-passed the company's mechanical billing system. In discussing Section 605, the *Brandon* court stated that "that provision was adopted by Congress for the protection of authorized users of telephonic or radio facilities" and that it did not apply to those who used the facilities without proper authority.

The *Brandon* interpretation of Section 605 should apply with equal force to the Omnibus Crime Act. There is no reason to believe that Congress in adopting the 1968 Act intended to establish a refuge for wrongdoers who illegally use communications facilities belonging to others. On the contrary, the legislative history of the Omnibus Crime Act makes it clear that Congress intended to give trespassers no refuge. Prior to the passage of the Act the following colloquy took place between Senator Murphy and Senator McClellan, the floor manager of the bill:

"Mr. MURPHY. There are now electronic devices available to the individual householder which he can buy and install to protect his home. One device I know of, in the case of an illegal entry by a burglar, immediately notifies the police, records the sounds and voice patterns of those who are improperly in that house.

"I should like to ask the Senator from Arkansas, will this device be permitted under Title III as it now stands?

"Mr. MCCLELLAN. Yes. In the home, or in the apartment, such a device would be permitted.

"I invite the attention of the Senator to pages 93 and 94 of Report No. 1097 where he will find:

" 'Paragraph (2)(c) provides that it shall not be unlawful for a party to any wire or oral communication or a person given prior authority by a party to a communication to intercept such communication. It largely reflects existing law. Where one of the parties consents, it is not unlawful. (*Lopez* v. *United States*, 83 S. Ct. 1381, 373 U.S. 427 (1963); *Rathbun* v. *United States*, 78 S. Ct. 161, 355 U.S. 107 (1957); *on Lee* v. *United States*, 72 S. Ct. 967, 343 U.S. 747 (1952)). Consent may be expressed or implied.

"Surveillance devices in banks or apartment houses for institutional or personal protection would be impliedly consented to. Retroactive authorization, however, would not be possible. (*Weiss* v. *United States*, 60 S. Ct. 269, 308 U.S. 321 (1939)) and "party" would mean the person actually participating in the communication. [sic] (*United States* v. *Pasha*, 332 F. 193 (7th), *Certiorari denied* 85 S. Ct. 75, 379 U.S. 839 (1964)).'

"If a burglar breaks into a house and his voice is recorded, he took that risk when he broke in there." 114 CONG. REC. S6209 (daily ed. May 23. 1968).

The Senate debates make it clear that a trespasser "impliedly" consents to the interception of his communications. In the facts of the present case, the ex-employee who used the Commission's telephone for personal calls did not expressly consent to the interception of his calls. Within the meaning of the Omnibus Crime Act he did, however, "impliedly" consent to such an interception. This consent is implied, as a matter of law, from the fact that he was a trespasser on the Commission's communications facilities. In the words of Senator McClellan "he took that risk" when he became a trespasser.

The preceding discussion makes it clear that an employer has every right to protect himself by monitoring his own telephones where they are being used by a non-employee without proper authorization. The cases decided under old Section 605 of the Communications Act indicate that, in certain circumstances, an employer is even entitled to protect his rights and property through the monitoring of *employee* calls.

In 1958, the Supreme Court of New Jersey considered the applicability of Section 605 to a case involving a conspiracy to steal the property of a leather company. *State* v. *Giardinia*, 27 N.J. 313, 142 A. 2d 609 (1958). One of the company's employees used its telephones to arrange for the delivery of the stolen property to a co-conspirator. These calls were monitored through the company switchboard, with the employer's authorization, but without the knowledge or consent of either party to the conversations. The Court, in *Giardinia*, held that the company did not violate Section 605 by monitoring the calls. The U.S.

Supreme Court's opinion in *Rathbun* v. *United States*, 355 U.S. 107 (1957), was quoted to the effect that it "is unreasonable to believe that Congress meant to extend criminal liability to conduct which is wholly innocent and ordinary." 142 A. 2d 609, 611. The New Jersey court felt that " . . . a criminal statute should not be invoked in defiance of the common sense of a situation . . ." and that "Congress could hardly have intended a sanctuary for criminals within the home or plant of their victim." 142 A. 2d 609, 611–12. It was believed that, in the facts of *Giardinia*, the subscriber's surveillance of his own lines was a "reasonable" and "normal" practice. 142 A. 2d 609, 612.

A federal court in *United States* v. *Beckley*, 259 F. Supp. 567 (N.D. Ga. 1965), came to a similar result. The *Beckley* court held that "Section 605 does not prohibit the telephone company from monitoring its own lines. 259 F. Supp. 567, 571. It was felt that the Communications Act:

". . . does not deprive the telephone company of the right to employ reasonable means to detect and prevent violations . . . by its own employees. Where, as is here alleged, a corrupt employee allows long distance calls to be covertly made without charge and in a manner which bypass the regular bookkeeping procedures of the company the only reasonable means of protection is the monitoring of such calls." *Ibid.*

The principles set out in *Beckley* were specifically incorporated into the Omnibus Crime Act. 18 U.S.C. §2511(2)(a); see also legislative history at 1968 U.S. Code Cong. & Ad. News 2112, 2182. The Act authorizes an employee of a communications common carrier to intercept wire communications where such interception ". . . is a necessary incident to the rendition of his service or to the protecting of the rights or property of the carrier." 18 U.S.C. §2511(2)(a). In addition to this exception for common carriers, the Act provides for an exception for switchboard operators. It appears, therefore, that the Act recognizes the holding in *Giardinia* as well as that of *Beckley*. The Act makes no specific mention of a subscriber's use of an *extension* to monitor his own lines. It does not appear, however, that there is any logical distinction between the use of a switchboard and the use of an extension where both are being utilized for an admittedly valid purpose. The 1968 Act, like old Section 605 of the Communications Act, should properly be interpreted in a common sense fashion. In the language of *Giardinia*, it must be assumed that Congress did not intend " . . . to denounce the reasonable and normal actions of a man in monitoring his own telephone lines to protect himself from others who use his lines without his authority in an effort to injure him." 142 A. 2d 609, 612.

There is certainly nothing in the leigslative history of the Omnibus Crime Act which would indicate that Congress "intended a sanctuary for criminals within the home or plant of their victim."

The foregoing analysis clearly indicates that the surveillance presently under consideration did not violate the Omnibus Crime Act. The legislative history of the Act makes it plain that a trespasser on someone else's communications facilities takes the risk that his conversation may be intercepted. Congress simply did not intend to establish a refuge for those who illegally use another man's telephones in an effort to injure him.

B. The Fourth Amendment

The Fourth Amendment to the Constitution prohibits "unreasonable" searches and seizures. This provision was considered in *Katz* v. *United States*, 389 U.S. 374 (1967), in the context of the electronic monitoring of a call from a public telephone booth. In establishing a constitutionally protected right of privacy, the Supreme Court held that "the Government's activities in electronically listening to and recording the petitioners words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." *Id.* at 512. The defendant in the *Katz* case was, of course, in a different position from the one occupied by the suspect in the case now being considered. The telephone booth in *Katz* was available for public use and anyone using it had a right to rely on the privacy of his calls. The suspect in the present case was in Commission offices after working hours and was without any proper authority to use the Commission's telephone lines.

It is well established that a trespasser, that is, one who is wrongfully present upon premises, has no right of privacy in those premises. *Jones* v. *United States*, 362 U.S. 457 (1960); *United States* v. *Gregg*, 403 F. 2d 222 (6th Cir. 1968), aff'd 394 U.S. 489 (1969); *United States* v. *Miller*, 449 F. 2d 974 (D.C. Cir. 1970); *Kaufman* v. *United States*, 323 F. Supp. 623 (E.D. Mo. 1971). In *Jones*, the Supreme Court stated that: ". . . anyone legitimately on premises where a

search occurs may challenge its legality. . . . This would of course not avail those who by virtue of their wrongful presence, cannot invoke the privacy of the premises search." *Jones* v. *United States*, *supra*, p. 267. A typical case involving trespassers was considered by the Supreme Court of Hawaii in 1961. *State* v. *Pokini*, 45 Hawaii 295, 367 F. 2d 499 (1961). The case involved a search of a vehicle which certain defendants were occupying illegally, having abducted the owner and converted his car to their own use. The Court held that the defendants, as trespassers, had no right of privacy in the automobile and that their Fourth Amendment rights were not violated by a search of the car or by a seizure of guns found under the front seat. It would seem to follow that the suspect in the present case, as a trespasser who was using Commission telephone lines in a way inimical to Commission interests, had no right of privacy which the Fourth Amendment would protect. The Supreme Court in the *Katz* case emphasized the fact that the defendant *justifiably* relied on the privacy of his calls. A trespasser—whether in someone else's car or on someone else's communications facilities—is not justified in placing any reliance on the privacy of his activities. Authority to search out a suspected trespasser should be especially broad where the search is conducted by the owner of the property or communications facilities being searched. To hold otherwise would be to give the trespasser a right to use the property free of any effective control by the true owner.

In the present case, even an employee would have no Fourth Amendment right of privacy in the calls which were made. These calls had a direct bearing on Commission business. The government, as a federal employer, has every right to supervise and investigate its employees *in the performance of their duties*. In *United States* v. *Collins*, 349 F. 2d 683 (2d Cir. 1965), cert. denied, 383 U.S. 960 (1966), the Second Circuit considered the search of a Customs Service employee's work area and desk. A package, last seen near the employee's desk, had been stolen from the mail. A search of the desk uncovered the contents of this package. The Court stated that:

"We have no doubt that the search of defendant's work area, including the surface and interior of his desk . . . was a constitutional exercise of the power of the Government as defendant's employer, to supervise and investigate the performance of his duties as a Customs employee. Defendant was handling valuable mail for which the Government was responsible. The agents were not investigating a crime unconnected with the performance of defendant's duties as a Customs employee." *Id.* at 867–68.

This principle would not, however, authorize searches of a work area where the purpose is to uncover facts unrelated to an employee's on-the-job duties. See *United States* v. *Block*, 188 F. 2d 1019 (D.C. Cir. 1951).

In addition to their duty of supervising employee performance, federal agencies are charged with a responsibility of maintaining a reasonable degree of order and security. In *United States* v. *Donato*, 269 F. Supp. 921 (E.D. Pa.) aff'd 379 F. 2d 288 (3rd Cir. 1967) a search of U.S. Mint employee's locker was justified as a reasonable means of maintaining order and security in the Mint. Here it was stated that:

"It is settled law that the Fourth Amendment does not prohibit reasonable searches when the search is conducted by a superior charged wtih the responsibility of maintaining discipline and order or of maintaining security." *Id.* at 730–31.

Searches designed to maintain institutional order or security have also been held reasonable in cases involving student dormitories, *Moore* v. *Student Affairs Committee of Troy State University*, 284 F. Supp. 725 (M.D. Ala. 1968), and Federal Job Corps Centers, *United States* v. *Coles*, 302 F. Supp. 99 (D.C. Me. 1969).

The authorities discussed above clearly indicates that the Fourth Amendment gives a non-employee "trespasser" no right of privacy on the Commission's lines. The cases also indicate that the Commission's duty to supervise its employees' performance and maintain security would permit the surveillance of certain of their calls.

CONCLUSION

For the reasons stated above, I am of the opinion that there was no violation of either the Omnibus Crime Control and Safe Streets Act or the Fourth Amendment to the Constitution.

JOHN W. PETTIT,
General Counsel.

May 15, 1972.

52

EXHIBIT E

FCC 61-1289 11355

FEDERAL COMMUNICATIONS COMMISSION, WASHINGTON, D.C.

ADMINISTRATIVE ORDER NO. 12

At a session of the Federal Communications Commission held at its offices in Washington, D.C., on the 25th day of October, 1961:

The Commission has under consideration the question of telephone monitoring without prior notification to the other party. It appears that the Commission has never had a policy which permitted such monitoring of telephone communications; however, a policy expressly prohibiting such monitoring has not heretofore been formalized in an administrative order or directive. In view of the foregoing and in order that the policy with respect thereto shall be made explicit

It Is Ordered, pursuant to Section 4 (i) and (j) of the Communications Act of 1934, as amended, that:

1. Telephone communications by or to officials and employees of this agency shall not be monitored by Commission personnel without prior notification to the other party.

2. No electronic, mechanical, or any other listening device shall be used in the Commission for the purpose of monitoring or interception of telephone conversations without the knowledge of both parties and the use of the recognizable repetitive beep tone during such recording as required by the Commission's Report in the Matter of Use of Recording Devices in Connection with Telephone Service, Docket No. 6787, dated March 24, 1947.

It Is Further Ordered, That this Order shall become effective immediately.

BEN F. WAPLE,
Acting Secretary.

EXHIBIT F

SEPTEMBER 8, 1970.

Hon. JOHN E. MOSS,
Chairman, Committee on Government Operations, House of Representatives, Washington, D.C.

DEAR MR. CHAIRMAN: This is with reference to your letter of July 29, 1970, requesting information pertinent to the current survey by the Foreign Operations and Government Information Subcommittee "of the telephone monitoring practices of Federal departments and agencies."

With respect to this Commission, there has been no change in the situation reported to your Subcommittee in Chairman Minow's letter to you of November 3, 1961: Administrative Order No. 12 (two copies of which are enclosed) is still in effect, and this Order prohibits Commission personnel from monitoring telephone communications without prior notification to the other party. Moreover, the Commission neither possesses nor utilizes any of the telephone recording devices referred to in questions two through five of your letter.

As to your first question, the "covert" monitoring of telephone conversations by "a secretary or any third person being on the line" is barred by Administrative Order No. 12. I am sure that within the agency there is occasional "overt" monitoring (i.e., where the other party is notified that a third person is on the line); however, I do not believe that this practice, even though permitted by Administrative Order No. 12, is a common one at this agency.

I trust that the above information satisfies your request, and we will, of course, supply any further information your Subcommittee may require for its current survey.

Sincerely,

DEAN BURCH,
Chairman.

Enclosure.

U.S. Internal Revenue Service. Inspection of returns by Federal agencies. U.S. Congress. House. Committee on Ways and Means. Subcommittee on Oversight. IRS operations and taxpayer assistance. Hearings, 94th Congress, 1st session. Feb. 27 and April 14, 1975. p. 72.

INSPECTION OF RETURNS BY FEDERAL AGENCIES

Section 6103(a) of the Internal Revenue Code provides that returns shall be open to inspection upon order of the President. Treasury regulations approved by the President, 26 CFR 301.6103(a)-1(e), (f), (g), and (h), provide that the Secretary of the Treasury or the Commissioner of Internal Revenue may permit the head of a Federal agency to designate an employee of his agency to inspect tax returns where necessary in connection with some matter officially before the agency. The request must be signed by the head of the agency (no lesser official may make the request) and state the official purpose, the name and address of the taxpayer whose returns are desired, the type of return and the taxable period, and the name and title of the employees designated to inspect the returns or receive the information. When requests meet all of these criteria, they are honored. If any one requirement is not met, the request is denied. If IRS has any reason to believe that the purpose stated is not a valid one, the requester is contacted for further information before a decision to honor the request is made.

Requests from the Department of Justice may also be signed by the Assistant Attorneys General of the various divisions and by United States Attorneys. We will deny access to tax returns if the reason given is for an investigation of a tax matter, other than a tax case referred by IRS to the Department of Justice, as such investigations are under the jurisdiction of the Internal Revenue Service. Following are copies of correspondence from two United States Attorneys and our replies, with identifying information deleted, showing typical reasons and the emphasis placed upon confidentiality by both Justice and the Service. In addition, Notice 129 is affixed to each return furnished. Also provided in the following charts are the number of requests for returns made by Federal agencies for calendar year 1974 and the number of taxpayers (individuals and corporations) involved, as well as a summary of reasons for the request.

IRS does not peruse the return prior to submission to the agency for the purpose of deciding whether it contains information pertinent to the reason for the request. It is screened, however, to remove documents which, if disclosed, might hinder a tax case and the administration of the tax law or might identify or tend to identify informants. In requests involving a number of taxpayers, IRS may deny the furnishing of copies of returns, but may extract and provide selected information from the returns. Also, we encourage the inspection of returns at an Internal Revenue Service office, when possible, rather than providing copies.

The Federal Bureau of Investigation is a part of the Department of Justice and not an independent agency, and the Director of the FBI does not have authority to make requests for tax returns or tax data, other than tax checks. Therefore, any requests for returns for use of the FBI must be made by the Attorney General, the Deputy Attorney General, or an Assistant Attorney General.

In addition to disclosure to Federal agencies, Section 6103(b) of the Internal Revenue Code and the regulations issued thereunder provide for access to tax return information by States. But only if the use is for State or local tax administration purposes will it be made available and then only to State tax officials who have been designated in writing by the Governor. At the present time we have Federal-State tax agreements for the exchange of tax information with all the States except Nevada and Texas, and with the District of Columbia, American Samoa, Guam, and Puerto Rico. The same degree of safeguards are instituted to prevent unauthorized or unwarranted disclosures of tax information to States as to Federal Agencies.

U.S. Internal Revenue Service. Inventory of mechanical and/or electronic devices in custody of the Intelligence Division and the Inspection Service's Internal Security Division. U.S. Congress. House. Committee on Government Operations. Subcommittee on Commerce, Consumer, and Monetary Affairs. Oversight hearings into the operations of the IRS. Hearings, 94th Congress, 1st session. May 14-July 31, 1975. pp. 415-416.

415

INVENTORY OF MECHANICAL AND/OR ELECTRONIC DEVICES IN CUSTODY OF THE INTELLIGENCE DIVISION AND THE INSPECTION SERVICE'S INTERNAL SECURITY DIVISION

Category:	Quantity
Miniature transmitters	100
Miniature recorders	37
Other tape recorders used for investigative purposes	88
Miniature receivers	42
Telephone induction coils	108
Video cameras	21
Amplifier/microphones	4
Miniature receivers with recorders	2
Miniature amplifiers	10

The above items are those reported to the Attorney General in our annual report. The chapstick-type microphones discussed during the hearings on June 20, 1975 are access equipment furnished with small communication-type transmitters and receivers (transceivers), and these microphones are not specifically identified on our inventory records. These microphones are not designed nor intended to be used to monitor conversations. These transceivers and accessories are used by special agents to inconspicuously maintain two-way communications with other special agents while on foot surveillance.

The microphones are of the push-to-talk type which means that the agent must depress a switch while talking. In addition, the microphones are not sensitive and must be placed close to the user's mouth (less than 12 inches) in order to function effectively. This lack of sensitivity is advantageous in a communication-type microphone because high levels of background noise (street traffic, etc.) are not picked up and transmitted. This feature makes the microphone extremely ineffective for surreptitiously monitoring conversations since highly sensitive microphones are needed to pick up all levels of conversation within the area covered.

As a result of a telephone inquiry to the field, our regional Intelligence offices have informed us that they have a total of 92 microphones of the type described above. These are located in 16 of our 58 district offices.

In addition, Intelligence has four (4) UHF radio transceivers. Although not surveillance equipment, the only purpose of these UHF transceivers is to monitor surveillance recordings from two UHF transmitters included in the list above.

Additional investigative equipment on inventory in Inspection's Internal Security Division includes:

Category:	Quantity
Binoculars (Includes 3 night vision attachments)	110
Cameras (Plus 53 special lenses, meters, and flash attachment)	110
Mobile car radios	102
Handie talkies	194
Base station radios	16
Telephone analysers	4

Miscellaneous—Microphones, voltmeters, battery chargers, bench equipment, audio filters, speakers, head sets, photo enlarging equipment.

The Intelligence Division's current inventory includes the following investigative equipment: (where applicable, this equipment is included in the summary shown at the beginning of this insert).

Category:	Quantity
Photocopiers	318
Microfilm reader-printers	516
Rotary microfilm cameras	467
Planetary microfilm cameras	15
High speed microfilm cameras	10
Microfilm readers	73
Radio base stations	63
Mobile radios and accessory items	726
Portable radios	597
Radio amplifiers	190
Radio chargers	121

Radio receivers	14
35-mm cameras	221
Tele lenses and electronic flash	216
4 x 5 press cameras	8
Movie cameras	26
Projectors	31
Minox cameras	33
Tessina cameras	23
Polaroid cameras	133
Instamatic cameras	19
6 x 7 camera	1
Reel tape recorders	338
Cassette tape recorders	1,451
Cassette transcribers	274
Binoculars	703
Binocular cameras	15
Scopes	85
Illuminated filters for check unscrambling	80
Light amplification scopes	8
Portable video outfits	13
Surveillance trucks	16

NOTE.—Many reel recorders disposed of—not yet reflected on inventory records.

NOTE.—Most of the items in the Intelligence inventory, such as cassette tape recorders, are not normally reported as electronic surveillance equipment as they are not used for monitoring or intercepting conversations.

Mr. ROSENTHAL. This sounds like the chapstick connection.

Mr. ALEXANDER. Mr. Chairman, we think that chapsticks are fine in their general place. We think that the Internal Revenue Service has a responsibility to conduct itself responsibly, and we are trying to do this right now and we are incurring heavy criticism in so doing.

We will be glad to find the list that appears to be missing here as to number. We are instituting tight controls as to location and as to use of those devices.

Mr. ROSENTHAL. Let me just ask. There are two other reports. You don't have the other two? You don't have the one on strike forces? You don't have that handy?

Mr. BATES. I don't have it.

Mr. ROSENTHAL. Why don't I give this one to you and the one on narcotics traffic? You can just give us the summary of each of them and what your findings were, how you went about it, and what you did.

Mr. DRINAN. Coming back to what you call "consensual surveillance"; namely, an IRS agent talking to someone's attorney, companion, or associate, this is not deemed to be wiretapping, it is "consensual" monitoring with the IRS agent being the only one who consents.

Is this widespread? Is this very common? No one needs permission to do this?

Mr. CLANCY. During the calendar year of 1973, the consensual telephone—I don't like to use the word "interception" because that connotes it is a wiretap—we do not——

Mr. DRINAN. But it is. I mean the consensual part is only on the part of the IRS, so that is a deceptive term to begin with, isn't it?

Mr. CLANCY. Yes, sir.

Mr. DRINAN. All right. If the IRS person is the only one who consents, that is not consensual.

U.S. Office of Telecommunications Policy. Executive Office of the President. Cable (report to the President). Jan. 14, 1974 (Washington, D.C.).

Recommendation 10: ***There should be strong legal and technical safeguards to protect individual privacy in cable communications.***

There has been justifiable concern over the possible invasions of privacy posed by the development of cable. For example, remote monitoring services, such as automatic meter reading, may be used by unauthorized persons for clandestine surveillance. Unauthorized persons could also misuse confidential, personal information conveyed by cable to data storage or processing centers. Furthermore, commercial enterprises, and perhaps local governments, would be able to keep track of every program a person watches or any information service he or she uses. This could cause a substantial "chilling" effect on the flow of information as well as a serious erosion of privacy. New technology could also make it possible to address selectively each cable subscriber and provide the means to inundate him with unwanted information.

The Committee considers the individual's ability to safeguard his personal privacy to be one of the most important goals of a free society. The law and the traditions of a society based on the initiative, responsibility and privacy of the individual require that technology serve, not erode, this goal.

Therefore, we recommend the adoption of legal safeguards to allow individual control over undesired communications and intrusions into the home. These safeguards could include sanctions against the distribution of material which the subscriber indicated he does not wish to receive or which he has not specifically requested. In addition to these safeguards, the constitutional and "common" law of privacy would also apply to cable and should be adapted and enforced by the courts. Finally, cable lends itself to use of technical safeguards, such as scrambling codes and locked channels. The FCC, in conjunction with other Government agencies, should develop and implement technical standards and requirements necessary to afford added protection of privacy in cable communications.

U.S. Postal Service. Mail covers (statement by William J. Cotter, Chief Postal Inspector). U.S. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Postal Facilities, Mail, and Labor Management. Postal Inspection Service's monitoring and control of mail surveillance and mail cover programs. Hearings, 94th Congress, 1st session. May 6-Nov. 5, 1975. pp. 46-52.

Mail cover

A mail cover is a relatively simple investigative or law enforcement technique. It involves recording the name and address of the sender, the place and date of postmarking, the class of mail, and any other data appearing on the outside cover of any class of mail matter in order to obtain information in the interest of (1) protecting the national security; (2) locating a fugitive; or (3) obtaining evidence of the commission or attempted commission of a crime. Mail is not delayed in connection with a mail cover, and the contents of first-class mail are not examined. As sanctioned by law, the contents of second- third-, and fourth-class mail matter may be examined in connection with a mail cover.

Development of mail cover regulations

It is uncertain exactly when the mail cover technique originated, although it would seem rather natural to utilize postmarks and return addresses in the investigation of crimes related to the use of the mails. The 1879 postal regulations were the first to contain an official statement concerning the use of postmarks and addresses for law enforcement purposes. These regulations authorized postmasters and other postal employees to furnish information "concerning the postmarks and addresses of letters" to "officers of the law, to aid them in discovering a fugitive from criminal justice." However, postal employees were strictly forbidden to delay or refuse the delivery of mail to the persons addressed. *Postal Laws and Regulations*, sec. 531 (1879 ed.) See also sec. 507 (1887 ed.)

The 1893 edition of the regulations contained a discussion of the postal patron's expectation of confidentiality in his use of the mail system. The regulation declared that postal employees were "furnished with the names and addresses upon letters and other articles of mail matter for the sole purpose of enabling them to make delivery thereof to the persons intended. Such names and addresses are to be regarded as confidential, and this confidence must be respected." *Postal Laws and Regulations*, sec. 462 (1893 ed.).

The prohibition against disseminating information concerning mail matter thus seems to be rooted equally in the individual's expectation of confidentiality in his use of the mails and the desire of the Post Office Department to protect the public against fraud and other abuses of the postal system. It also appears to have been made clear from the beginning that information on matter entrusted to the mails could be released to serve an important public purpose, such as the apprehension of a fugitive from justice.

Subsequent revisions of the postal regulations continued to authorize postmasters to furnish "information concerning mail matter" to Postal Inspectors and to furnish postmarks, addresses, and return cards (return addresses) to officers of the law to assist them in locating fugitives. In addition, to serve important public needs or to insure the effective functioning of the postal system, the developing regulations made several carefully circumscribed exceptions to the confidentiality of address information. By stages, postmasters were authorized to release information to State agricultural inspection personnel, to correct mailing lists sent to them for revision, to testify in court regarding mail matter, and to furnish change of address information. However, access to the type of information obtainable from what are now known as mail covers was still limited to Postal Inspectors and officers of the law. *Postal Laws and Regulations*, sec. 549 (1902 ed.), sec. 523 (1913 ed.), sec. 508 (1924 ed.), sec. 702 (1932 ed.), and sec. 702 (1940 ed.). These personnel, however, were encouraged not to make unnecessary use of the procedure. *Manual of Instructions for Post Office Inspectors*, sec. 13.2 (July 1, 1941 ed.).

The 1948 regulations considerably broadened the access to mail cover information by allowing postmasters to furnish for official use, "upon official request of a representative of another executive department, agency, or independent establishment of the Federal Government and the presentation of proper credentials * * * information regarding the addresses, return cards, or postmarks on mail matter * * * *Postal Laws and Regulations*, sec. 41.4(b) (1948 ed.). Similar provisions were contained in the *Manual of Instructions for Postal Personnel*, Chapter XIV, sec. 1 and 3 (1948 ed.). These regulations, allowing mail covers to be requested by both law enforcement officers and representatives of any federal agency, were in effect in the early 1950s when mail covers first became a matter of Congressional concern. *Post Office Manual*, Chapter XIII, sec. 1 and 3 (1952 and 1954 eds.), and as revised by Old Manual Circular 5, January 10, 1955.

47

In 1952, members of the staff of the Senate Subcommittee on Privileges and Elections, which was investigating the conduct of Senator Joseph R. McCarthy, obtained covers on the mail addressed to the Senator and his aides. During the consideration of a resolution of censure against Senator McCarthy, the Senate authorized an investigation into the use of mail covers on his mail. S. Res. No. 332, 83d Cong., 2d Sess. (1954); 100 Cong. Rec. 16274–16277, 16331–16333, 16342–16344, 16350–16352, 16400, 16404 (1954). The special investigating committee recommended that the matter be referred to the Attorney General for possible action under the criminal statutes dealing with delay and obstruction of the mails, 18 USC secs. 1701–1703. However, the investigators found no evidence that mail covers had been maintained against any other members of the Senate. S. Rep. No. 2510, 83d Cong., 2d Sess. (1954); and 101 Cong. Rec. 2564 (1955).

As a part of the general revision of postal regulations which was accomplished in the years 1954 and 1955, the Post Office Department discarded the provisions allowing postmasters to furnish information concerning postmarks, addresses, and return cards to representatives of federal agencies. The new regulations once again limited the availability of such information to Postal Inspectors and officers of the law seeking fugitives from justice. *Postal Manual*, secs. 311.6 and 311.7 (1954 ed., Postal Procedures Transmittal Letter 6, August 10, 1955). An additional section charged postmasters to treat mail cover requests "in strict confidence," and warned that delivery of the mail should not be delayed in obtaining the information. *Postal Manual*, sec. 831.44 (1954 ed., Organization and Administration Transmittal Letter 7, July 31, 1956).

Thus, after approximately 76 years, the postal regulations applicable to the mail cover procedure still exhibited much of their original form, and access to mail cover information was once again limited to Postal Inspectors and law enforcement officers seeking to apprehend fugitives from justice.

Nevertheless, ten years later mail covers were again a topic of Congressional concern in the Senate hearings on invasion of privacy by government agencies. A Senate Subcommittee headed by Senator Edward V. Long of Missouri conducted extensive hearings on the use of mail covers. *See* Hearings on Invasions of Privacy (Government Agencies) Before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, 89th Cong., 1st Sess. (1965).

There was also sentiment for increased regulation or abolition of mail covers in the House of Representatives, where Mr. Cunningham introduced legislation similar in part to measures introduced by Senator Long (S. 2627, 88th Cong., 2nd Sess. (1964); S. 973, 89th Cong., 1st Sess. (1965)). H.R. 7709, 89th Cong., 1st Sess. (1965).

On June 17, 1965, the Post Office Department issued new regulations controlling the use of mail covers in Postal Bulletin No. 20478. The new regulations only allowed mail covers to be used in the interest of protecting the national security, locating a fugitive, or obtaining evidence of the commission or attempted commission of a felony. The regulations also required all mail covers to be authorized by the Chief Postal Inspector, a Postal Inspector in Charge, or a limited number of their designees. Moreover, mail covers were to be instituted only upon written request stipulating and specifying a reasonable need for the mail cover and a proper reason for its use. Other new provisions, apparently designed to counter specific changes in the Senate hearings, prohibited mail covers on matter mailed between a subject and his known attorney, placed time limits on all mail covers, and barred the continuation of mail covers on indicted persons. *Postal Manual* §§ 861.1 through 861.9 (1954 ed., Organization and Administration Transmittal Letter 112, August 11, 1965). In keeping with the tighter control over mail covers under the new regulations, § 311.7 was also amended to inform postmasters of the requirement that all mail covers must be authorized by the Chief Postal Inspector or a Postal Inspector in Charge. *Postal Manual* § 311.7 (1954 ed., Postal Procedures Transmittal Letter 173, July 27, 1965).

Revised mail cover regulations appeared to deal in a satisfactory manner with the potential for abuse present under the old provisions. Postmaster General John A. Gronouski declared:

"The new procedures are designed to protect a beneficial investigative and law enforcement technique from any possible abuse. I believe the new regulations will fully protect the rights of the innocent, while providing assistance in bringing to justice those who would prey upon the innocent." Post Office Department General Release No. 73, June 15, 1965.

In a law review article discussing the hearings, Senator Long testified to the Subcommittee's effectiveness in obtaining improved regulations and procedures concerning mail covers:

"New and more rigid controls have been issued in regard to the use of mail covers. Basically these regulations limit their use to investigations of crimes normally constituting a felony. Only the Chief Postal Inspector and District Postal Inspectors can order mail covers to be placed and only in defined situations, and only upon compliance with specific procedures. Indiscriminate use of mail covers that invade normally confidential relationships has been curbed. Records will be kept for a period long enough to make them available when needed in court, or administrative proceedings. Definite time limits have been set on the duration which a mail cover can be in effect.

"Additionally, a public understanding exists between the Subcommittee and the Postmaster General that if these new regulations are ignored, violated, or abolished, the Subcommittee will renew its push to outlaw mail covers completely." Long, *The Right to Privacy: The Case Against the Government*, 10 St. Louis Univ. L. J. 1, 25 (1965).

A subsequent law review writer, although opposed to retaining the mail cover procedure, admitted with regard to the new provisions, "The 32-paragraph order covered virtually all objections that had theretofore been raised." *Invasion of Privacy: Use and Abuse of Mail Covers*, 4 Columbia Journal of Law and Social Problems 165, 173 (1968).

Although Senator Long again introduced legislation to ban mail covers in the 90th Congress, S. 1061, 90th Cong., 1st Sess. (1967), the new postal regulations apparently shelved mail covers as an item of controversy. However, when the *Postal Manual* was replaced as the basic publication of postal regulations and instructions by the new *Postal Service Manual*, the regulations governing mail covers were not reprinted in their entirety. New § 233.2 contained a definition of the mail cover process, a statement of the permissible uses of mail covers, and a specification that only the Chief Postal Inspector or his designee could order mail covers. *Postal Service Manual*, § 233.2 (1970 ed., Organization and Administration Transmittal Letter 1, October 1, 1970.) Although omitted from the formal published regulations of the Postal Service, the extensive provisions of §§ 861.1 through 861.9 of the *Postal Manual* were retained as official instructions to all Postal Service employees and constituted the sole authority and procedure for initiating, processing, placing and using mail covers.

Most recently, the Postal Service has taken steps to republish the mail cover regulations in the *Postal Service Manual* and the *Federal Register* in order to make these regulations more accessible to the public and to discourage confusion concerning the nature and uses of this important investigative technique. In this republication, the Postal Service has updated the provisions dealing with the delegation of mail cover authority to reflect the present organizational structure of the Postal Inspection Service. However, no substantive changes have been made in mail cover procedures. 40 Fed. Reg. 11579–11580 (March 12, 1975).

Present mail cover regulations

The use of mail covers is now governed by regulations conveniently located under one heading in the *Postal Service Manual*. These regulations provide procedural and substantive safeguards designed to ensure the confidentiality of the mail cover process and prevent the unjustified use of mail covers. Among the most important of these safeguards are the following:

"Mail covers are to be used only in order to obtain information in the interest of (1) protecting the national security, (2) locating a fugitive, or (3) obtaining evidence of commission or attempted commission of a crime." (*Postal Service Manual* § 232.221.)

"No officers or employees of the Postal Service other than the Chief Postal Inspector and a limited number of his designees, are authorized to order mail covers." (*Postal service Manual* § 233.241.)

"Mail covers are ordered pursuant to a written request from a law enforcement agency only if the requesting authority stipulates and specifies the reasonable grounds that exist which demonstrate the mail cover is necessary to protect the national security, locate a fugitive, or obtain information regarding the commission or attempted commission of a crime. Only the Chief Postal Inspector, or his designee, may order a national security mail cover." (*Postal Service Manual* § 232.242b.)

"Mail covers are not to include matters mailed between the mail cover subject and his known attorney-at-law." (*Postal Service Manual* § 232.262.)

"Except in fugitive cases, no mail cover is to remain in force when the subject has been indicted for any cause." (*Postal Service Manual* § 232.266.)

"Any data concerning mail covers is to be made available to any mail cover subject in any legal proceeding through appropriate discovery procedures." (*Postal Service Manual* § 232.274.)

These present administrative safeguards over the use of mail covers furnish ample protection for the privacy of users of the mail.

Mail covers and the courts

A mail cover, like the "shadowing" of a suspect or an interview with the victim of a crime, is an investigative tool in the evidence gathering process—a means by which a law enforcement agency may develop significant facts to establish the probable cause necessary to obtain a search warrant or wiretap order or to make an arrest.

The Postal Service has long contended that it would be improper to extend to the mail cover, an investigate technique, the same type of judicial supervision reserved for law enforcement actions which may be properly described as "searches" or "seizures."

The Postal Service position on this matter is bolstered by the decisions of a number of respected courts which have uniformly refused to treat the mail cover technique as a search or seizure, or to extend the protections of the Fourth Amendment to matter inscribed on the outside of a piece of mail by the sender or by the Postal Service. The fundamental difference between the protected matter inside a piece of first-class mail and the unprotected matter on the cover of the mail was first stated by Mr. Justice Field:

"* * * [A] distinction is to be made between different kinds of mail—between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined. Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, *except as to their outward form and weight*, as if they were retained by the parties forwarding them in their own domiciles."

* * * * * * *

"Whilst regulations excluding matter from the mail cannot be enforced in a way which would require or permit an examination into letters, or sealed packages subject to letter postage, without warrant, issued upon oath or affirmation, in the search for prohibited matter, they may be enforced upon competent evidence of their violation obtained in other ways; *as from the parties receiving the letters or packages*, or from agents depositing them in the post-office, or others cognizant of the facts." *Ex parte Jackson*, 96 U.S. 727, 733, 735 (1877). (Emphasis added.)

Modern recognition of Justice Field's distinction between protected and unprotected mail matter was furnished in *Oliver* v. *United States*, 239 F. 2d 818 (8th Cir. 1957), *petition for cert. dismissed per stipulation*, 353 U.S. 952 (1957). The court stated:

"* * * [I]t seems to us that the discussion in [Jackson] * * * was primarily purposed to make it doctrinally clear that, in the Government's monopolistic right to provide the public with mail facilities, it could not escape the guaranties of the Bill of Rights, and that as to the search-and seizure guaranty of the Fourth Amendment it would be required to recognize a distinction between 'what is intended to be kept free from inspection' and 'what is open to inspection.'" 239 F. 2d at 821.

The principle of *Jackson* was explicitly applied to mail covers in *United States* v. *Costello*, 255 F. 2d 876 (2d Cir. 1958), *aff'g* 157 F. Supp. 461 (S.D.N.Y. 1957), *cert. denied*, 357 U.S. 937 (1958). Discussing the government's use of a mail cover, the court stated:

"In *Ex parte Jackson* * * *, the Supreme Court's discussion shows that a distinction is to be drawn between material which is sealed and material which is open for inspection. *We think the Jackson case necessarily implies that without offense to Constitution or statute writing apearing on the outside of envelopes may be read and used.* There seems to be a similar implication in *Oliver* v. *United States*, * * *: certainly that case does not suggest that the law is otherwise," 255 F. 2d 876 at 881. (Citations omitted, emphasis added.)

The Court of Appeals thus refused to disturb the following portion of the lower court's decision:

"It was not prying into their business or secrets to note what the senders had made public on the face of the letters."

* * * * * * *

"Any delay here was merely incidental to a lawful watch authorized by the postal regulations."

"The evidence shows no violation of Costello's rights under the Fourth Amendment." 157 F. Supp. 461 at 471. (Footnote omitted, emphasis added.)

Further explicit recognition of the constitutionality of mail covers has been afforded in *United States* v. *Schwartz*, 283 F. 2d 107, 111 (3d Cir. 1960), *aff'g* 176 F. Supp. 613 (E. D. Pa. 1959), *cert. denied*, 364 U.S. 942 (1961); *Canaday* v. *United States*, 354 F. 2d 849, 856 (8th Cir. 1966); *Cohen* v. *United States*, 378 F. 2d 751, 760 (9th Cir. 1967), *aff'g* 251 F. Supp. 269 (N. D. Cal. 1965), *cert. denied*, 387 U.S. 917 (1967); *Lustiger* v. *United States*, 386 F. 2d 132 (9th Cir. 1967), *cert. denied*, 390 U.S. 951 (1968); and *United States* v. *Isaacs*, 347 F. Supp. 743, 750 (N.D. Ill. 1972), *aff'd, rehearing denied*, 493 F. 2d 1127 (7th Cir. 1974), *cert. denied*, 417 U.S. 976 (1974).

Opening of mail

First-class mail is protected by the Fourth Amendment of the U.S. Constitution. First-class mail is matter closed against postal inspection. Title 39, Code of Federal Regulations, 131.2(a)(1)(iv).

Title 39, United States Code, § 3623(d) provides in part, "The Postal Service shall maintain one or more classes of mail for the transmission of letters sealed against inspection. * * * No letter of such a class of domestic origin shall be opened except under authority of a search warrant authorized by law, or by an officer or employee of the Postal Service for the sole purpose of determining an address at which the letter can be delivered, or pursuant to the authorization of the addressee." Moreover, improper opening of first-class mail or mail tampering can subject an individual to serve criminal penalties. 18 U.S.C. §§ 1701–1703, 1709. Part 115 of the *Postal Service Manual* (codified as § 115.1 of title 39, Code of Federal Regulations) provides: "First-class mail is given absolute secrecy while in our custody. No persons in the Postal Service, except employees of dead-mail offices, may open first-class mail without a legal warrant, even though it may contain criminal or otherwise unmailable matter or may furnish evidence of the commission of a crime." Although § 3623(d) of title 39 speaks only of letters, packages closed against inspection are afforded the same protection under postal regulations. Title 39, Code of Federal Regulations § 131.2(a)(3)(iii) provides: "Matter closed against inspection includes mail of any class so wrapped as not to be easily examined, except second-, third-, or fourth-class matter sealed subject to postal inspection."

The leading case in this area is *Ex parte Jackson*, 96 U.S. 727 (1877). In this case, a unanimous court held that although Congress had broad power over the nation's postal system, including the right to determine what shall be excluded from the mails, government policies exercising that power must be enforced "consistently with rights reserved to the people, of far greater importance than the transportation of the mail.

"* * * Letters and sealed packages [intended to be kept free from inspection] in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guarantee of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household." 96 U.S. 733.

The Court's distinction between what is "intended to be kept free from inspection" and what is "open to inspection" has been consistently followed ever since. The Court recently referred to this distiction with approval in *U.S.* v. *Van Leeuwen*, 397 U.S. 249 (1970). The Court in this case held that postal officials may detain suspicious first-class mail for a reasonable time while an investigation and an application for a search warrant are made.

A legally authorized search warrant is required to open and search first-class mail. Furthermore, under its current mail classification system and regulations, the Postal Service does not subject to a warrantless search any item which the sender has mailed air mail, air parcel post, or priority mail, except in those cases where such mail bears a notation by the sender authorizing postal examination.

Even in those cases where probable cause exists to believe there is contraband in first-class mail, e.g., damaged mail exposing contraband or other reliable information, a search warrant must be obtained without causing an unreasonable delay to the suspect mail. Although exposure of contraband through accidental damage to mail may be used as probable cause for a search and seizure warrant, the mail may not be withdrawn for use as evidence in a criminal proceeding without following the search warrant procedure.

A search warrant authorized by Rule 41 of the Federal Rules of Criminal Procedure may be issued upon receipt of a request from a federal law enforcement officer or an attorney for the government. Under Rule 41(h), the Attorney General has designated the Postal Inspection Service as one of the agencies authorized to request search warrants. However, only in the rare emergent case is a Postal Inspector permitted to seek a search warrant without the concurrence of the U.S. Attorney's office.

Dead letters

Section 159.7 of title 39, Code of Federal Regulations defines dead mail as matter deposited in the mail which is or becomes undeliverable, or is unmailable, and which cannot be returned to the sender. At dead letter branches, dead first-class letters are opened in an attempt to determine the name and address of the sender so that his property may be returned. Only those employees especially designated to open dead letters are allowed to open such matter and then only under proper supervision. Letters which contain correspondence only and which are without sufficient information to enable a return to the sender or delivery to the addressee are destroyed.

Second-, third-, and fourth-class mail

Matter which is "intended to be kept open to inspection" within the meaning of *Ex parte Jackson* clearly includes second-, third-, and fourth-class mail under present postal regulations. Second-, third-, and fourth-class mail are subject to postal inspection by authorized postal employees. Title 39, Code of Federal Regulations, § 125.2(e); §§ 134.8 and 135.7.

Payment of postage at the rates established for these classes of mail is considered consent by the sender to examination of the mail contents since the sender is free to choose the greater privacy of first-class mail. The courts have perceived no constitutional impediment to warrantless searches of these classes of mail. *Santana* v. *U.S.*, 329 F. 2d 854 (1st Cir. 1964); *Webster* v. *U.S.*, 92 F. 2d 462 (6th Cir. 1937).

Subsequent decisions by federal courts of appeal have been consistent with *Jackson* and have merely adjudicated whether particular mail items were intended to be kept free from postal inspection. *Oliver* v. *U.S.*, 239 F. 2d 818 (8th Cir. 1957); *Santana* v. *U.S.*, *supra*. Although second-, third-, and fourth-class mail may be opened for inspection, if such inspection discloses contraband, a search warrant must be obtained prior to the seizure of the item or withdrawal from the mails for use as evidence against the sender in a criminal proceeding.

Perhaps it should also be pointed out that pursuant to Customs laws (19 USC 1582, as implemented by § 162.2 of title 19, Code of Federal Regulations), mail of foreign origin is subject to customs inspections. Postal regulations recognize such foreign mail is subject to customs inspections without regard to class. Section 61.1 of title 39, Code of Federal Regulations. The most recent case of which we are aware upholding the right to subject foreign originating mail to a customs search is *United States* v. *Odland*, 502 F. 2d 148 (7th Cir. 1974).

Enactment of legislation requiring court orders for a mail cover

You also requested the views of the Postal Service on legislation which would require prior court approval of the use of a mail cover. For a number of reasons the Postal Service believes that it is inappropriate to require a court order prior to the placing of a mail cover.

First and foremost, the Postal Service feels it is improper and unreasonable to extend a probable cause standard required for a search and seizure to the mail

cover, an investigative and law enforcement technique concerned only with information published on the outside of an envelope and thus clearly beyond the protective scope of the Fourth Amendment. This opinion is supported by an impressive line of court decisions which have consistently refused to equate a mail cover to a search and seizure or to extend Fourth Amendment protections to matter written on the outside wrapper of a piece of mail by the sender or inscribed thereon by the Postal Service. In this connection your attention is invited to the discussion entitled "Mail Covers and the Courts", *supra*.

The substitution of a probable cause standard is unnecessary in light of the administrative standards and safeguards currently governing the imposition of a mail cover. As indicated above, a request for a mail cover must stipulate and specify in writing the reasonable grounds that exist which demonstrate the mail cover is necessary to protect the national security, locate a fugitive or obtain information regarding the commission of a crime or attempted commission of a crime (felony). It must cite the statute and the possible penalty involved and whether the subject has been indicted or has an attorney. The grounds upon which the need for a mail cover is based must be specific in order to permit a determination that the essential requirement is met. Mail covers cannot be authorized for exploratory purposes.

The sufficiency of a mail cover request is the heart of the mail cover regulations. It is the Postal Service and, in particular, the Chief Inspector who bears all responsibility as to whether approved requests are in keeping with the regulations. The request becomes a permanent part of the mail cover file which must be made available through appropriate discovery procedures in any legal action. The subject of a mail cover would thus be able to challenge not only the propriety of the judgment of the postal official imposing the mail cover, but also the truthfulness and sufficiency of the statements filed by the authority requesting the mail cover.

In our estimation the probable cause standard should be reserved for police actions such as searches, wiretaps, and arrests, which clearly infringe upon the privacy, security, and freedom of an individual. Applying the probable cause standard to a mail cover, which is often used in ascertaining whether there is probable cause to support a search or an arrest, would limit the usefulness and availability of an important investigative technique and would impair the ability of law enforcement personnel to deal with a variety of criminal activities. In our view, it would be as improper to apply the probable cause standard to a mail cover as it would be to apply that standard to the physical observation of a suspect.

Furthermore, the Postal Service believes that from a practical standpoint it would be undesirable to impose upon a request for a mail cover the same requirements of probable cause and specificity applied to an application for a search and seizure warrant. The Inspection Service investigates a wide variety of mail fraud schemes, many of which prey directly on individual consumers. These cases require prompt investigative attention to determine the legitimacy of an operation or the scope and victims of a questionable one. In this regard it has been our experience that the mail cover investigative technique has proved itself many times over as a means of establishing the scope of a fraudulent scheme, the identity of the operators, and, equally important, identity in a timely manner of persons being victimized by the scheme long before they would be aware of the fraudulent nature of the operation. In all probability Postal Inspectors would not be able to establish probable cause for the establishment of a mail cover in the early stages of certain mail fraud schemes. This would be particularly true in "fly by night" operations. The unavailability of a mail cover on a timely basis would not only compromise efforts to identify those being victimized and to ascertain the scope of a fraudulent operation, but might also enable a fast-moving fraud artist to evade effective investigation altogether. As a result, Postal Inspectors would face unnecessary difficulties in their efforts to develop the evidence to support an arrest of the perpetrator of a mail fraud and to secure the return of money taken from defrauded consumers. The Postal Service feels that applying a probable cause requirement to the use of mail covers in mail fraud investigations would seriously hamper our efforts to protect the American consumer.

For the reasons stated above, the Postal Service is of the opinion that no legislation concerning mail covers is necessary at this time. We believe that the legitimacy of mail covers has been established by indisputable judicial precedents, that existing postal regulations contain insurance against the abuse of mail covers, and that subjecting mail covers to statutory constraints similar to those designed for searches and seizures would be both improper and impractical.

B. Commissions

U.S. Commission on CIA Activities Within the United States. Report. Washington, D.C.: U.S. Govt. Print. Off., June 6, 1975: 3-9

Chapter 1

The Fundamental Issues

In announcing the formation of this Commission, the President noted that an effective intelligence and counterintelligence capability is essential to provide "the safeguards that protect our national interest and help avert armed conflicts."

While it is vital that security requirements be met, the President continued, it is equally important that intelligence activities be conducted without "impairing our democratic institutions and fundamental freedoms."

The Commission's assessment of the CIA's activities within the United States reflects the members' deep concern for both individual rights and national security.

A. Individual Rights

The Bill of Rights in the Constitution protects individual liberties against encroachment by government. Many statutes and the common law also reflect this protection.

The First Amendment protects the freedoms of speech and of the press, the right of the people to assemble peaceably, and the right to petition the government for redress of grievances. It has been construed to protect freedom of peaceable political association. In addition, the Fourth Amendment declares:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .

In accordance with the objectives enunciated in these and other Constitutional amendments, the Supreme Court has outlined the following basic Constitutional doctrines:

1. Any intrusive investigation of an American citizen by the government must have a sufficient basis to warrant the invasion caused by the particular investigative practices which are utilized;

4

2. Government monitoring of a citizen's political activities requires even greater justification;

3. The scope of any resulting intrusion on personal privacy must not exceed the degree reasonably believed necessary;

4. With certain exceptions, the scope of which are not sharply defined, these conditions must be met, at least for significant investigative intrusions, to the satisfaction of an uninvolved governmental body such as a court.

These Constitutional standards give content to an accepted principle of our society—the right of each person to a high degree of individual privacy.

In recognition of this right, President Truman and the Congress—in enacting the law creating the CIA in 1947—included a clause providing that the CIA should have no police, subpoena, law-enforcement powers or internal security functions.

Since then, Congress has further outlined citizen rights in statutes limiting electronic surveillance and granting individuals access to certain information in government files,[1] underscoring the general concern of Congress and the Executive Branch in this area.

B. Government Must Obey the Law

The individual liberties of American citizens depend on government observance of the law.

Under our form of Constitutional government, authority can be exercised only if it has been properly delegated to a particular department or agency by the Constitution or Congress.

Most delegations come from Congress; some are implied from the allocation of responsibility to the President. Wherever the basic authority resides, however, it is fundamental in our scheme of Constitutional government that agencies—including the CIA—shall exercise only those powers properly assigned to them by Congress or the President.

Whenever the activities of a government agency exceed its authority, individual liberty may be impaired.

C. National Security

Individual liberties likewise depend on maintaining public order at home and in protecting the country against infiltration from abroad

[1] Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. Secs. 2510–20) and Privacy Act of 1974 (5 U.S.C. Sec. 552a).

and armed attack. Ensuring domestic tranquility and providing for a common defense are not only Constitutional goals but necessary preconditions for a free, democratic system. The process of orderly and lawful change is the essence of democracy. Violent change, or forcing a change of government by the stealthy action of "enemies, foreign or domestic," is contrary to our Constitutional system.

The government has both the right and the obligation within Constitutional limits to use its available power to protect the people and their established form of government. Nevertheless, the mere invocation of the "national security" does not grant unlimited power to the government. The degree of the danger and the type of action contemplated to meet that danger require careful evaluation, to ensure that the danger is sufficient to justify the action and that fundamental rights are respected.

D. Resolving the Issues

Individual freedoms and privacy are fundamental in our society. Constitutional government must be maintained. An effective and efficient intelligence system is necessary; and to be effective, many of its activities must be conducted in secrecy.

Satisfying these objectives presents considerable opportunity for conflict. The vigorous pursuit of intelligence by certain methods can lead to invasions of individual rights. The preservation of the United States requires an effective intelligence capability, but the preservation of individual liberties within the United States requires limitations or restrictions on gathering of intelligence. The drawing of reasonable lines—where legitimate intelligence needs end and erosion of Constitutional government begins—is difficult.

In seeking to draw such lines, we have been guided in the first instance by the commands of the Constitution as they have been interpreted by the Supreme Court, the laws as written by Congress, the values we believe are reflected in the democratic process, and the faith we have in a free society. We have also sought to be fully cognizant of the needs of national security, the requirements of a strong national defense against external aggression and internal subversion, and the duty of the government to protect its citizens.

In the final analysis, public safety and individual liberty sustain each other.

Chapter 2

The Need for Intelligence

During the period of the Commission's inquiry, there have been public allegations that a democracy does not need an intelligence apparatus. The Commission does not share this view. Intelligence is information gathered for policymakers in government which illuminates the range of choices available to them and enables them to exercise judgment. Good intelligence will not necessarily lead to wise policy choices. But without sound intelligence, national policy decisions and actions cannot effectively respond to actual conditions and reflect the best national interest or adequately protect our national security.

Intelligence gathering involves collecting information about other countries' military capabilities, subversive activities, economic conditions, political developments, scientific and technological progress, and social activities and conditions. The raw information must be evaluated to determine its reliability and relevance, and must then be analyzed. The final products—called "finished intelligence"—are distributed to the President and the political, military and other governmental leaders according to their needs.

Intelligence gathering has changed rapidly and radically since the advent of the CIA in 1947.[1] The increased complexity of international political, economic, and military arrangements, the increased destructiveness of the weapons of modern warfare, and the advent of electronic methods of surveillance have altered and enlarged the needs for sophisticated intelligence. Intelligence agencies have had to rely more and more on scientific and technological developments to help meet these needs.

Despite the increasing complexity and significance of intelligence in national policymaking, it is also important to understand its limits. Not all information is reliable, even when the most highly refined

[1] The CIA is only one of several foreign intelligence agencies in the federal government. Others include the National Security Agency, the Defense Intelligence Agency, the intelligence branches of the three military services and the State Department's Bureau of Intelligence and Research.

intelligence methods are used to collect it. Nor can any intelligence system ensure that its current estimates of another country's intentions or future capacities are accurate or will not be outrun by unforeseen events. There are limits to accurate forecasting, and the use of deception by our adversaries or the penetration of our intelligence services increases the possibility that intelligence predictions may prove to be wrong. Nevertheless, informed decision-making is impossible without an intelligence system adequately protected from penetration.

Therefore, a vital part of any intelligence service is an effective counterintelligence program, directed toward protecting our own intelligence system and ascertaining the activities of foreign intelligence services, such as espionage, sabotage, and subversion, and toward minimizing or counteracting the effectiveness of these activities.

Foreign Invasions of United States Privacy

This Commission is devoted to analyzing the domestic activities of the CIA in the interest of protecting the privacy and security rights of American citizens. But we cannot ignore the invasion of the privacy and security rights of Americans by foreign countries or their agents. This is the other side of the coin—and it merits attention here in the interest of perspective.

Witnesses with responsibilities for counterintelligence have told the Commission that the United States remains the principal intelligence target of the communist bloc.

The communists invest large sums of money, personnel and sophisticated technology in collecting information—within the United States—on our military capabilities, our weapons systems, our defense structure and our social divisions. The communists seek to penetrate our intelligence services, to compromise our law enforcement agencies and to recruit as their agents United States citizens holding sensitive government and industry jobs. In addition, it is a common practice in communist bloc countries to inspect and open mail coming from or going to the United States.

In an open society such as ours, the intelligence opportunities for our adversaries are immeasurably greater than they are for us in their closed societies. Our society must remain an open one, with our traditional freedoms unimpaired. But when the intelligence activities of other countries are flourishing in the free environment we afford them, it is all the more essential that the foreign intelligence activities of the CIA and our other intelligence agencies, as well as the domestic counterintelligence activities of the FBI, be given the support neces-

sary to protect our national security and to shield the privacy and rights of American citizens from foreign intrusion.

The Commission has received estimates that communist bloc intelligence forces currently number well over 500,000 worldwide.

The number of communist government officials in the United States has tripled since 1960, and is still increasing. Nearly 2,000 of them are now in this country—and a significant percentage of them have been identified as members of intelligence or security agencies. Conservative estimates for the number of unidentified intelligence officers among the remaining officials raise the level to over 40 percent.

In addition to sending increasing numbers of their citizens to this country openly, many of whom have been trained in espionage, communist bloc countries also place considerable emphasis on the training, provision of false identification and dispatching of "illegal" agents—that is, operatives for whom an alias identity has been systematically developed which enables them to live in the United States as American citizens or resident aliens without our knowledge of their true origins.

While making large-scale use of human intelligence sources, the communist countries also appear to have developed electronic collection of intelligence to an extraordinary degree of technology and sophistication for use in the United States and elsewhere throughout the world, and we believe that these countries can monitor and record thousands of private telephone conversations. Americans have a right to be uneasy if not seriously disturbed at the real possibility that their personal and business activities which they discuss freely over the telephone could be recorded and analyzed by agents of foreign powers.

This raises the real specter that selected American users of telephones are potentially subject to blackmail that can seriously affect their actions, or even lead in some cases to recruitment as espionage agents.

Chapter 3

Summary of Findings, Conclusions, and Recommendations

As directed by the President, the Commission has investigated the role and authority of the CIA, the adequacy of the internal controls and external supervision of the Agency, and its significant domestic activities that raise questions of compliance with the limits on its statutory authority. This chapter summarizes the findings and conclusions of the Commission and sets forth its recommendations.

A. Summary of Charges and Findings

The initial public charges were that the CIA's domestic activities had involved:

1. Large-scale spying on American citizens in the United States by the CIA, whose responsibility is foreign intelligence.
2. Keeping dossiers on large numbers of American citizens.
3. Aiming these activities at Americans who have expressed their disagreement with various government policies.

These initial charges were subsequently supplemented by others including allegations that the CIA:

—Had intercepted and opened personal mail in the United States for 20 years;

—Had infiltrated domestic dissident groups and otherwise intervened in domestic politics;

—Had engaged in illegal wiretaps and break-ins; and,

—Had improperly assisted other government agencies.

In addition, assertions have been made ostensibly linking the CIA to the assassination of President John F. Kennedy.

It became clear from the public reaction to these charges that the secrecy in which the Agency nesessarily operates, combined with the allegations of wrongdoing, had contributed to widespread public misunderstanding of the Agency's actual practices.

U.S. Commission on the Organization of the Government for the Conduct of Foreign Policy. Intelligence support for foreign policy in the future (prepared by Russell Jack Smith). Vol. 7, Appendix U, Washington, D.C.: U.S. Govt. Print. Off., 1975: 84–86.

Innovations in Intelligence Support

Both within the intelligence agencies and outside among their customers there is a constant desire to improve the ways in which intelligence information is transmitted. Intelligence people are constantly experimenting with new ways to convey the printed word, new uses for graphic displays, new devices for getting and holding the attention of the policy reader. On the other end, policy desk people are always looking for greater impact from intelligence reports; they ask for some means to alert them more fully or inform them more thoroughly. Because the techniques by which policy people ingest information are highly individualistic and because novelty in presentation has inherent appeal, albeit relatively short-lived, a continuous program of experiment and change seems both inevitable and desirable.

Among the avenues for improvement, the use of electronic data processors and video tube display devices have been most thoroughly explored. It has been expected by some that these modern machines will soon displace typewritten reports and the printed word. It has been urged that in this age of instant communication and high speed decision, policy people can no longer be served adequately with printed reports but must be provided with "real time" information relayed directly from the scene of action to their desks. It has also been suggested that government has been laggard in recognizing the advance of modern technology in this field.

The intelligence agencies, spurred both by this criticism and by their own recognition of the need for greater speed in handling their information, have been experimenting with a variety of machines for processing and transmitting information for over a decade and have been conducting intensive research and development for five years or so. Also, they have called in top experts from the national communications media to study ways of improving their procedures. By so doing they have established some guiding concepts for present and future applications, and they have reached the stage where pragmatic use of machine processing on a large scale can begin.

Among the guiding concepts that have emerged from these studies are these: (a) people currently in top policy positions are not prepared either by background or training to receive essential information by visual display or computer read-out instead of the printed word; (b) the information essential to the support of policy—intensively worked data, reasoned and modulated judgments, interlocking analyses of causes and dynamics—do not lend themselves to electronics and are better transmitted in printed paragraphs; and (c) tremendous advances can be made in the speed and efficiency with which information is processed by intelligence analysts using machines precisely designed to their needs.

Difficult as it is to generalize about the backgrounds of people in top foreign policy positions, it is still probably fair to say that gen-

erally their training has been more in economics, political science, and law than it has been in mathematics and the physical sciences. They have formed twin habits of acquiring information from the printed page and expressing themselves in written papers. Although they may have had some experience with modern computers, they usually have not performed serious work directly with the machines, as have their counterparts in the hard sciences. The information they customarily handle consists largely of approximations, generalizations, and judgments—not the discrete, quantitative data which adapts readily to digital expression. They have been trained to think in words, not numbers, and the policy work they do finds expression in words.

Moreover, except when they are dealing with a sharp crisis—say, an invasion of the Middle East—their work does not call for a steady series of high speed decisions. Most policy determinations require deliberate and intensive study before action. It is largely a myth that modern communications demand instant decisions and a twenty-four hourly readiness to react. Modern communications permit, or facilitate, quick response but they do not in themselves require it.

Crisis situations, on the other hand, do usually require rapid decision and response, and here the intelligence agencies must be prepared to use all the resources of modern technology to assist that process. For the most part, the technology already exists and what is needed is the investment of resources. Among future means of speeding the decision-making process will be video relays from television cameras on the site of crucial meetings or other key developments and televised briefings by intelligence experts who are interpreting information as fast as it arrives.

But even here, only a little reflection is needed to realize that these situations will be the exception, not the rule. Top policy people seldom have the need, and even more seldom have the time, to follow a crisis step by step as it unfolds. They must instead rely on summarized and gisted information from assistants while they spend much of their time in policy meetings and discussions with their fellow policy makers.

Although the need is clear for occasional availability of "real time" service for top policy people, the greater need is for electronic passage of information to desk officers in policy organizations and for machine processing of information for intelligence analysts. It is here that the future looks most promising for effective work.

Over the past three years substantial progress has been made in identifying precisely which phases of analytic work are adaptable to machines and in designing machines to do that work. The key to this substantial progress has been that the machines have been patterned around the work analysts actually do, not the other way around. Very often the advocates for machine data processing have lacked any intimate understanding of the work being done. They have known that machines can perform a great variety of high speed operations and they have assumed that the work can be readily adapted to the specific requirements of the machines. Prolonged experimentation has demonstrated that this is not always true. Most of the materials which intelligence analysts handle resist strict codification or digitalization. More often it is descriptive, approximative, or judgmental.

One task which intelligence analysts perform daily is to read "the traffic," the flow of cables, reports, and telegrams which reach their desk in staggering volume. A great deal of effort has been expended on speeding up this process with electronic machines, and it is now clear that in the future analysts will use text processing machines for this chore. One such system would display incoming cables on the analyst's desk, machine-sorted appropriately for his individual mission and coded by number. Scanning these cables on the video tube before him, the analyst could select those items he would like to have delivered to his desk for more intensive study and comparison with other material. This system will not only speed the process of moving innumerable bits of information around the organization, but it will also sharply reduce the consumption of paper and facilitate a corresponding reduction in the size of analysts' files.

Another system just coming into use which will be widely available for broad application in the future is a text searching machine. This system stores information in such a way that it is retrievable by key phrases punched on a console on an analyst's desk. It can provide the sentence in which the key phrase, or proper name, appears, and can provide sentences both immediately preceding and succeeding. This context enables the analyst to decide whether he needs to see the full report or can reject it. This system has the greatest utility for handling information which is easily codified, such as tabulated election results or lists of targets covered by photographic reconnaissance. Because material of this kind tends to have a high proportion of dross to metal and also comes in prodigious batches, this system will go a long way toward freeing the analyst for more useful work.

These are two examples of the adaptation of electronic machines to analytic intelligence work. Their number could be added to now and certainly will be multiplied in the future. It is fair to say that automatic data processing, appropriately designed for the specific tasks and specialized materials of intelligence work, can be a widespread reality in the next five years.

Other innovations in intelligence support are most likely to come in new formats and new conceptual approaches. Aside from those employing electronics, however, it is difficult to predict their exact shape. There has always been a steady series of adjustments and accommodations by intelligence to the expressed desires of the policy readers. The morning current intelligence report for President Kennedy moved through a steady progression from a simple listing of new reports to a highly literate account of the developments interspersed with analytic judgments, all changes being made in response to direct suggestion by the President. Similarly, the daily report was made a late afternoon publication for President Johnson who liked his ready at the end of the day. Again, the daily summary was returned to a morning timing for President Nixon, and a sharp line was drawn between fact and judgment in response to his request.

National estimates have recently undergone redesign in response to criticism by high level readers. There has been a move away from the broad consensus approach and treatment which was developed to meet the needs of the National Security Council under President Eisenhower. In its place has developed a national intelligence estimate

79-064 O - 76 - 30

more directed toward the delineations of issues and options, a change largely responsive to current modes and procedures introduced by Secretary of State Kissinger to the National Security Council.

As suggested above, the outlook is for a continuing series of such changes, made in response to the changing shape and texture of problems policy confronts. What will be required to ensure that intelligence provides optimum support for policy in the future is the sustaining of a dialogue which will permit precise tailoring of intelligence to needs. Both parties need to take an aggressive posture in this respect. The experience of the past, which has sound application for the future, is that policy people are often unaware that intelligence has something highly pertinent to say about their current concerns, while intelligence is unwittingly pursuing strands and facets of lesser value. There is a remedy for this. It consists of regular, frequent, and frank discussion between intelligence and policy people about present and emergent policy problems and the available or obtainable information which can be brought to bear on those problems.

U.S. Commission on the Organization of the Government for the Conduct of Foreign Policy. Problems in the conduct of United States foreign policy: a compilation of recent criticism (prepared by J. Daniel O'Flaherty). Vol. 7, Appendix X. Washington, D.C.: U.S. Govt. Print. Off., 1975: 335.

C. SCIENCE AND TECHNOLOGY

(1) Foreign policy agencies of the government, especially State, are poorly equipped to deal with science and technology. The Office of the Special Assistant for Science and Technology, set up in 1962, was too insulated from public and congressional scrutiny, was moved to the Executive Office where it became preoccupied with domestic policy, and was a "scientific fire brigade." There is a demonstrated need for greater scientific advice within the agencies (Skolnikoff).

(2) The International Science Committee, set up under the Federal Council for Science and Technology and chaired by State, failed to develop or articulate uniform policies. State is a prisoner of the views and desires of the technical agencies, not a source of independent policy. The International Scientific and Technological Affairs Office in State failed to involve itself in foreign aid, disarmament and military matters, and did little more with respect to policy affecting NASA and the AEC (Skolnikoff).

(3) U.S. scientific and technological policy toward Western Europe is *ad hoc*, partly because there is no place in the government where concerted science and technology policy is formulated. United States R&D should be done in review with Western Europe and other developed countries (Haskins, Basiuk).

U.S. Federal Advisory Committee on False Identification. Proposed findings and recommendations. Federal Register. v. 41, no. 117. June 16, 1976: 24431–24437:

FEDERAL ADVISORY COMMITTEE ON FALSE IDENTIFICATION

Proposed Findings and Recommendations

The purpose of this announcement is to provide the public with a final opportunity to comment on the proposed findings and recommendations of the Federal Advisory Committee on False Identification (FACFI) All comments will be considered by the Committee before taking final action on its report. Comments of particular interest will be summarized in the Committee's final report to be issued this Summer. The Committee is merely a fact finding group. Thus, its recommendations have no force of law.

Comments should be made in writing and sent on or before July 7, 1976 to:

David J. Muchow, Chairman, Federal Advisory Committee on False Identification, Department of Justice, Washington, D.C. (Telephone: 202–739–2745.

In addition to a full analysis of the scope of the false identification problem and recommended solutions, the Committee's final report will include: an analysis of Federal and State legislation dealing with false identification; proposed Federal and state legislation to combat false identification; proposed guidelines for state plans to control access to vital statistics records and control issuance of birth certifications; standardized forms for birth certificates, a program for the matching of birth and death certificates; and a program for upgrading the security of state drivers' licenses. Also included will be reports from each of the Committee's five task forces; several background papers including: (1) an overview of electronic funds transfer systems (EFTS); (2) a summary of automated identification technology; (3) a summary of fraud resistant identification verification techniques; (4) a survey of national systems for personal identification; and a number of special studies.

I. The Purpose

FACFI was established by the Attorney General under the Federal Advisory Committee Act (Pub. L. 92–463, 5 U.S.C. Appendix I.) in November 1974 to: (1) study the nature and scope of the criminal use of false identification; and (2) to recommend measures, consistent with personal privacy, to combat such use at Federal, state and local levels and in the commercial and private sectors. The Committee's charter may be found in the Federal Register of October 23, 1974.

The Committee consists of approximately 75 representatives from some 50 agencies, the commercial sector and the public. The Committee has conducted its business in monthly meetings in Washington, D.C. All of the Committee's meetings have been open to the public and the Committee welcomes a broad spectrum of comments from the public to assist it in its efforts to increase personal privacy and to aid in preventing the criminal use of false identification.

II. Definition of False Identification

The Committee has defined "false identification" as the intentional use by an individual of a document containing a name or personal attributes other than his own for the purpose of assisting in the commission of a crime or in avoiding the legal consequences of a previous crime. This definition is broad enough to encompass the use of a forged check to obtain cash or other benefits, even if no supporting documentation is demanded by the victim of the transaction. It also includes the use of false identity documents for noncriminal transactions by an escaped convict or other individual sought under a fugitive warrant.

The identity documents (IDs) with which the FACFI has been concerned include not only commonly used IDs such as birth certificates, driver's licenses, passports, employee badges, and military identification cards, but also documents whose major purpose is other than identification of the bearer, e.g., personal and government checks and credit cards. Any of these documents can be and is often used to support a false identity.

III. How False IDs Are Obtained

False identity documents can be obtained readily and inexpensively anywhere in the United States or neighboring countries from a variety commercial sources or by "do-it-yourself" techniques. In any large city one can find photo studios that provide customers with photo ID cards replete with official-looking signatures and seals in any name, address or birthdate of the customer's choice—no questions asked. Thriving mail-order businesses, which advertise their services nationally through "underground" newspapers and magazines, supply blank birth certificates and baptismal certificate forms and mount customer-supplied photographs on counterfeit "state ID" cards. Dozens of document vendors south of the U.S. border sell counterfeit U.S. immigration documents and border crossing cards for whatever the traffic will bear. Most of these activities are beyond the reach of current Federal or state laws.

Pickpockets and purse snatchers find a ready market for stolen IDs, especially checkbooks, credit cards, and driver's licenses. However, the enterprising imposter has no real need to risk the use of counterfeit or stolen documents; he can obtain all the genuine ID's he needs in any number of false names from the legal issuing offices themselves. The methods for obtaining genuine documents in false names have become widely known in recent years. Possession by a criminal of a full set of genuine IDs in a false name is known in law enforcement circles as the "infant death identity", or IDI, syndrome.

The first step in establishing an IDI is obtaining a certified copy of the birth certificate of a person who was born about the same date as the imposter but who died in early childhood. The information the imposter requires to apply for such a certificate (more properly called a certification of birth) is generally the name, exact date, and place of birth of the deceased infant. This information can be obtained from old newspapers or from local birth records themselves where

public access to such records is permitted. Posing as the person described on the certificate, an imposter can obtain certification through the normal process of writing to the registrar of births; more brazen imposters can get quicker service by applying in person at a state or local Vital Records Office.

A birth certificate is an extremely valuable document to an imposter. If he is an alien, for example, the certification gives him the ability to enter the U.S. unquestioned and to enjoy all the rights of citizenship. Furthermore, the falsely obtained certificates can be used as a "breeder" document to construct a completely new identity. In this case the imposter uses the certification as "proof" of identity to obtain a state driver's license (or state ID card) and a Social Security Number. The license is the de facto U.S. ID for check cashing and other commercial transactions; together with the birth certificate, it can be used to apply for a U.S. passport. A Social Security number opens the door to most employment or public assistance; once this is accomplished, the imposter need only establish a minimal credit rating to apply for credit cards. He is then free to enjoy (or abuse) all the credit and social benefits of U.S. life with impeccable credentials in a false name. And, he can assume, either sequentially or in parallel, other false identities by the same method.

This ruse is highly successful for several reasons. First, application for a deceased person's certification is unlikely to attract suspicion because birth and death records are handled by separate offices and are seldom correlated. Secondly, the birth certificate is almost always accepted as validation of the name and citizenship of the bearer, even though it contains no physical description (except for sex and possibly race) of the person whose birth it records. Finally, the imposter runs little risk of punishment in obtaining the certification under false pretenses because in many states it is legal to apply for and to possess another person's birth certificate even for fraudulent purposes. It is of course illegal to use such a document to support false claims of citizenship or to apply for other official documents.

IV. The Scope of the False ID Problem

Possession of false identity documents gives a criminal the means to "appear" and "disappear" almost at will and without a trace. Firm statistics on the scope and impact of crimes aided by false ID are difficult to obtain. In general, the use of false ID is a modus operandi and thus is not recorded as a separate crime. False identification fraud is in many cases an "invisible" problem that is recognized only after careful investigation. Thus, for example, the magnitude of false identification fraud in public assistance programs can be estimated only from the results of a handful of local studies. Even on the basis of this sparse data, however, it is apparent that the criminal use of false identification represents a multibillion dollar problem in the United States. The figures obtained by the FACFI are conservative and represent the tip of a criminal iceberg.

The false identification problem impacts nationally in six major problem areas as summarized in Table 1.

TABLE 1.—SUMMARY OF SCOPE AND IMPACT OF NATIONAL FALSE IDENTIFICATION PROBLEM

Problem area	Scope of problem	Extent of false ID use	Source of data
Drug smuggling	Over $1,000,000,000 per year	80 pct of hard drugs smuggled	Customs Service, Drug Enforcement Administration, Passport Office.
Illegal immigration	Over $12,000,000,000 per year.[1]	Unknown; used in entry, employment, welfare application.	Immigration and Naturalization Service, independent studies.
Evasion of justice	Over 300,000 fugitives per year.	Close to 100 pct of Federal cases.	FBI, sheriffs, and police survey.
Fraud against business	Over $3,000,000,000 per year.[2]	Over $1,000,000,000 per year	American Bankers Association, independent studies.
Fraud against government.	Unknown	Over $140,000,000 per year [3]	Surveys of welfare officials, published studies.
Other criminal activity	do	Very common	FBI, sheriffs, and police survey.

[1] Estimated U.S. tax burden.
[2] Includes out-of-pocket losses and cost of collection attempts.
[3] Based on sparse data; includes theft of welfare checks and false ID applications.

1. *Drug Smuggling.*—Approximately 80% of the hard drugs entering the United States is smuggled by organized rings that make extensive use of false identification. The "street value" of these drugs is estimated to be approximately $1 billion per year, which does not include the loss incurred by government and private citizens for the value of goods stolen by addicts or the costs of addict rehabilitation. Passports obtained and used fraudulently facilitate the flow of drugs and aliens across U.S. borders.

2. *Illegal Immigration.*—The tax burden caused by the presence of illegal aliens in the United States has been estimated by independent consultants to the Immigration and Naturalization Service to be in excess of $12 billion per year. This burden represents the costs of public services and welfare benefits to the extent they are not supported by taxes paid by the aliens, and includes the indirect costs related to the job displacement of U.S. citizens by illegal aliens. We cannot be certain how much of this staggering burden can be attributed to the use of false IDs by illegal aliens, but we believe it is substantial and increasing.

3. *Fugitives From Justice.*—Escaped prisoners and other dangerous fugitives almost always obtain false IDs to avoid detection and capture. In a recent FBI survey of 500 names of wanted persons chosen at random, all had active aliases. In recent years, a number of notorious fugitives have been able to escape arrest for considerable periods of time in part because of the effectiveness of their false IDs. While the FACFI is unable to estimate the cost of false ID use by fugitives, we do emphasize that the ability of dangerous criminals to move freely and undetected in society is a serious threat to public safety.

4. *Fraud Against Business.*—Our findings indicate that the use of false IDs is costing American business well over $1 billion each year. Fraud against business includes check forgery and fraud, credit card fraud, securities fraud, and embezzlement. A substantial part of these fraud losses is due to the use of false ID's by counterfeiters, forgers and imposters. Check fraud hits particularly hard at retail food stores and small businesses. The average food store is estimated to suffer losses of over $7,000 per year through false ID fraud.

Banks suffer losses primarily through forgery of stolen checks; these losses were estimated by the American Bankers Association at $50 million for 1974. While the bank losses are not as significant as the check fraud losses suffered by other forms of business, they far exceed the total losses due to bank robbery and burglary combined.

The most common type of false identification fraud involving credit cards is the use of stolen cards by imposters; other forms include the use of counterfeit credit cards or application for cards in a false name by a person with criminal intent. We have been unable to secure estimates of fraud losses from the credit card organizations themselves; however, a 1974 Department of Commerce publication placed losses on bank credit cards from all sources at approximately $500 million per year.

5. *Fraud Against Government.*—Surveys conducted among state and Federal welfare officials by the FACFI revealed that there are no uniform standards for the identification of welfare recipients. Thus, we have no way to estimate the scope of multiple collection of benefits by individuals using several identities. Losses from false identities could well number in the billions of dollars. A New York District Attorney who found several cases of such fraud in a single welfare center concluded that illegal multiple entitlement is "the most serious problem faced in the administration of Public Assistance and one for which there are no present adequate safeguards." [1] Significant evidence of the use of false IDs in obtaining illegal benefits was also uncovered in an investigation of the Food Stamp Program in Arkansas. Further investigation of false identification welfare fraud in many more locations is necessary, however, before the national impact of this problem can be accurately estimated.

In Philadelphia, before a serious effort was made in 1974 to reduce the mailing of welfare checks, an average of 10,000 replacements for checks reported "lost or stolen" were issued each month. About 41% of the lost or stolen checks were subsequently forged, resulting in an annual loss of $4.8 million. A similar audit of lost or stolen checks conducted in the New York City found forgery losses to be in excess of $8 million during the year ending October 1973. Forgery of stolen benefit checks—amounting to approximately $10 million during 1975—appears to be a major source of loss to Federal Social Security programs.

6. *Other Criminal Activity.*—The foregoing examples illustrate major categories of crimes where the criminal's success is dependent in large measure on the ease with which he can obtain false identification. However, the usefulness of false IDs has not been lost on the common criminal engaging in crimes ranging from confidence games to house burglary. In his response to a FACFI survey a Dayton, Ohio sheriff sums it up:

> The growing and thriving business in underworld sale of false identification adn related items has become so standard that not only does the common thief have ready access to any type of false ID he wishes, but also he finds the going street price within easy reach of his budget.

[1] "Report on Investigation of Welfare Fraud for 1974," Ferraro, N., District Attorney, Queens County, N.Y., 1975.

V. Response to the Problem

The FACFI has been charged not only with documenting the problem of criminal use of false identification, but also with developing written proposals for dealing with it at all levels of government as well as educating the public in ways to reduce such crimes. To accomplish these goals, the FACFI has been holding regular sessions in Washington, D.C. since November 1974. All meetings have been announced in advance in the Federal Register and have been open to the public. The FACFI and its staff have examined a large number of potential solutions to false ID problems received from FACFI members, survey respondents, and members of the general public. Other ideas for solutions were gleaned from newspaper and magazine articles, testimony before Congress, and the experience of other democratic societies in dealing with problems of identification. Information was also requested from vendors of fraud-resistant identity verification devices and techniques through a solicitation published in the Commerce Business Daily.

Members of the FACFI evaluated potential solutions through a formal procedure and then ranked them with respect to criteria that included an assessment of effectiveness and potential impact on public convenience and privacy.

We recognize the legal and implied rights to privacy and the threat to those rights by excessive government interference. Thus, FACFI has maintained a careful balance in formulating recommendations for dealing with the national false identification problem; we have considered both protection against crime and protection of privacy to be guarantees provided to all in a free society.

VI. Proposed Findings and Recommendations

1. *The question of a National Identification Document.*—The concept of a uniform personal identification document, to be issued and secured by Federal or state government, has occasionally been proposed as a sweeping solution to the problems of false identification. National IDs are in fact used by a number of nations with democratic traditions as well as those under other forms of government. The FACFI considered it necessary and advisable to study the national ID concept as carefully and rationally as possible in order to illuminate the advantages and problems inherent in such an approach.

Three different approaches to a system of uniform personal identification were evaluated by FACFI members. One approach proposed a federally-issued document designed specifically for personal identification with the U.S. This document would be available to citizens on a voluntary basis and would incorporate application procedures and security features similar to those used in the U.S. passport. The second suggestion envisioned a complete national identification system in which citizens would be registered at birth. This proposal included an automated verification system—a data base containing only identity information—that could be accessed only by the registered individual to verify his identity to government agencies. The third proposal suggested the use of present state driver's licenses (and "non-driver"

state IDs) as recognized and required personal identification. Application for such a document would be required of all citizens at age 16. Safeguards against counterfeiting, alteration, and use by imposters would have to be included in all such state documents.

Similar arguments can be brought to bear in favor of and against all these proposals. Arguments in favor of a single standardized type of ID include the belief that:

Such a document could be more easily recognized, controlled and protected against abuse.

Document systems that include everybody would thereby be "foolproof".

Government has an obligation to provide a reliable means of personal identification for public and private transactions among its citizens.

Arguments against a standardized national ID include the belief that such documentation is in opposition to American tradition and would represent an invasion of personal privacy, and that data required for citizen identification could be abused by government or private interests.

It is certain that any new system designed to verify and store identity information on over 200 million people would be extremely expensive and require a major national effort. It is highly probable that proposals for such a system would be opposed politically. If such a system were implemented despite these difficulties, it would be subject to defeat by imposters or counterfeiters taking advantage of careless inspection of documents or through corruption of officials. Occasional errors would also occur in such a system that could adversely affect innocent people.

The FACFI therefore strongly opposes any new type of state, or local government-issued ID intended to supersede existing documents. In short, FACFI opposes any so called "National ID card."

The FACFI instead recommends that the security of existing state document systems be increased, particularly for breeder documents such as the birth certificate and the driver's license. Security must be increased both in the application phase (during which documents are issued) and in the use phase (when the documents are used).

Thus, the aim of FACFI's recommended Federal actions is to insure the increased security and privacy of existing state identification documents in state, interstate, and Federal transactions.

The following recommendations are designed to accomplish this goal of increased security for state documents. FACFI findings in each case are also included to permit association with the recommendations.

2. *Right to Privacy.*—The FACFI finds that the criminal use of false identification often invades personal privacy; that innocent citizens are victimized when their good names and credit are used in criminal transactions; and that the protection of personal privacy is an essential right, fully consistent with sound law enforcement efforts to reduce false identification crimes.

The FACFI therefore recommends that individual privacy rights be given the fullest consideration in the formulation and implementation of the following legislative and administrative proposals to counter the criminal use of false identification.

3. *Birth Certificates.*—The FACFI finds that certified copies of birth certificates have frequently been abused by imposters and counterfeiters because:

Unsigned requests by mail for such documents are usually honored.
The birth certificates of deceased persons are not usually so designated.
Records of deaths and births in many states are open for "browsing" by persons seeking false identification.
Minimum standards are not available for issuance security and document security of birth certifications.
Some 7,000 local vital records offices are autonomous in the format, seals, and safeguards provided for their certifications.

Information on the abuse of birth certificates is often not given to the proper state authorities.

Abuse of birth certificates is not sufficiently covered by legislation at either the state or Federal level.

The FACFI therefore recommends that: a Fraudulent application be discouraged by use of state-issued standard application forms requiring the applicant's signature, justification of request, and items of personal history not generally available to imposters.

b. A system be implemented for intrastate and interstate matching of birth and death records to note the fact of death on the birth certificates of all persons aged 55 years or less at the time of death.

c. State laws to protect individual privacy by limiting public access to birth and death records be enacted in all states lacking such legislation.

d. Minimum standards for identification of applicants for birth certification, and for security of certified copies against theft, alteration and counterfeiting be drafted for adoption by states.

e. Federal agencies that require personal identification in application for privileges or benefits accept as primary evidence of age and place of birth only those U.S. birth certifications issued by a state or state-controlled records office.

f. Formal notification of the abuse of a birth certification be given by state and Federal law enforcement agencies to the appropriate state registry officials. The information exchange can be facilitated through the establishment of a clearinghouse for false ID information.

g. Wherever practical, requests for birth certificates be retained by the issuing office to assist in the detection and tracing of fraudulent requests.

h. Appropriate state and Federal legislation be enacted to prohibit the fraudulent application for, possession, sale, and transfer of birth certifications for the purpose of establishing a false identification.

4. *Driver's Licenses.*—The FACFI finds that state driver's licenses (and "nondriver" state ID or "age-of-majority" cards) are frequently abused by counterfeiting, imposture, or fraudulent application because:

They are used as personal ID for commercial transactions and dealings with government agencies although this use was not intended by issuing authorities.
Because the security of issuance procedures and of the document itself varies widely among the states.
Driver's licenses and other State identification documents are not sufficiently protected by Federal legislation against interstate abuse.

The FACFI therefore recommends that: a. The state-issued driver's license (or state-issued ID) be recognized as the primary form of

personal ID for use in commerce and in general transactions between individuals and government.

b. Guidelines be drafted by the Federal government providing minimum standards for the identification of applicants for original, replacement, or interstate exchange of driver's licenses and state IDs, and for security of those documents against counterfeiting, alteration, and use by imposters.

c. Voluntary compliance by all states with these guidelines be encouraged by appropriate Federal funding or other incentives and/or sanctions.

d. An analysis and implementation plan for improvement in the security of state ID systems be developed by the Law Enforcement Assistance Administration (LEAA) for consideration by the states.

e. Federal legislation be enacted to prohibit counterfeiting in any state of personal IDs issued by any other state, and to prohibit use of the channels of interstate commerce to assist fraudulent application for state IDs.

5. *Drug Smuggling.—The FACFI finds* that smuggling of narcotics and other dangerous drugs by criminal organizations is aided materially by extensive use of false U.S. and foreign passports and other documents.

The FACFI therefore recommends that: a. Birth certificates and state-issued ID, as the primary documents used in U.S. passport application procedures, be secured in accordance with FACFI recommendations.

b. Federal agencies concerned with the activities of drug smuggling (including the Immigration and Naturalization Service, Drug Enforcement Administration, Customs Service, Passport Office, and Visa Office) provide coordinated training programs for the detection of false IDs used by smugglers and communicate frequently with each other and state and local authorities on the observed patterns of such false ID use.

c. Interpol be encouraged to coordinate international law enforcement efforts in the detection of passport fraud.

6. *Illegal Immigration.—The FACFI finds that illegal aliens* routinely use false IDs such as stolen or counterfeit immigration documents and border crossing cards, and U.S. birth certificates and voter registration cards obtained under false pretenses, to enter and remain in the United States. By obtaining Social Security accounts, they are able to secure employment to which they are not entitled, made easier because knowing employment of illegal aliens is not prohibited under Federal law.

The FACFI therefore recommends that: a. The Immigration and Naturalization Service (INS) be provided with sufficient funds to develop and implement an improved system for registration of legal aliens that will resist attempts at forgery, counterfeiting, and use of INS documents by imposters.

b. Birth certificates and secondary evidence of U.S. citizenship be secured in accordance with foregoing FACFI recommendations.

c. Identification and citizenship of applicants for new Social Security accounts be verified by stricter evidentiary requirements or other appropriate means.

d. Federal legislation be enacted to counteract knowing employment of illegal aliens.

7. *Fugitives From Justice.—The FACFI finds* that dangerous fugitives are able to avoid apprehension through the use of false identification, and that, when arrested they may be released before their identity and criminal history are confirmed.

The FACFI therefore recommends that: a. State and Federal document systems be protected from abuse by fugitives through enactment of FACFI recommendations for birth certificates and driver's licenses.

b. State laws be enacted requiring verification of the identity of all persons arrested, prior to their release on bond.

c. To meet such identification requirements without endangering arrestees *habeas corpus* rights, appropriate equipment be used for highspeed transmission of fingerprints and other identifying data between local law enforcement offices and state identification bureaus.

8. *Fraud Against Business.—The FACFI finds* that American business is subjected to billion-dollar losses each year from false identification fraud through forgery and counterfeiting of personal and corporate checks, impersonation based on stolen credit cards, and negotiation of lost or stolen securities.

The FACFI therefore recommends that: a. The business community make use of improved technological safeguards against false ID fraud.

b. The business community participate in the increasing development and use of electronic funds transfer systems, which have the potential of reducing false ID fraud by reducing the amount of negotiable paper in circulation. The potential for privacy abuses and significant false ID fraud via electronic manipulation must be addressed in the design of such systems.

c. The security of driver's licenses and other state IDs, which are widely used in commercial transactions, be improved through implementation of FACFI recommendations.

9. *Fraud Aganist Government.—The FACFI finds* that government programs such as public assistance Food Stamps and Social Security are subjected to unacceptable annual losses through false identification fraud and that such fraud results principally from the use of false IDs at application for benefits and in the cashing of stolen benefit and payroll checks.

The FACFI therefore recommends that: a. The Federal government draft uniform standards for the identification of applicants for federally supported or cost-shared public assistance programs.

b. Mailing of welfare and payroll checks to individual addresses be superseded by mailing or direct deposit to banks and thrift institutions to the extent that such depositing is beneficial to recipients and practical.

c. The identity of applicants for new Social Security accounts be verified by stricter evidentiary requirements or other appropriate means.

d. Cooperative programs be instituted for the training of welfare and Social Security employees in techniques for detection and reporting of the use of false identification.

e. The security of birth certificates and driver's licenses which are frequently used in application for government payments be improved through implementation of FACFI recommendations.

10. *False Identification Data.—The FACFI finds:* a. That many government agencies and companies who regularly are being defrauded by false identification schemes are not aware that they are being victimized. This is because false identification crimes are often not detected until long after the crime has been committed.

b. That there is almost a total lack of meaningful statistics concerning false identification crimes both in government agencies and the commercial sector; there is great reluctance by organizations to reveal these crimes even which they are discovered because such losses are embarrassing to the organizations concerned; and that such failure to expose the criminal use of false identification has contributed to the proliferation and success of this criminal technique.

The FACFI therefore recommends: a. That Federal, state and local agencies and the commercial sector develop increased awareness of the nature of false identification crimes, compile statistics on those crimes which are committed within their organizations, and affirmatively seek methods of preventing the commission of such crimes both in the "application stage" (when fraudulent applications are made) and in the "use stage" (when false documents are improperly used).

b. That Federal, state and local law enforcement agencies and firms in the commercial sector establish a statistical base line by which to measure the increase or decrease in false identification crimes. And that other data on false identification be complied including the type of crime, modus operandi, and a profile of the user and victim of false statistics relating to false identification crimes to be published in Uniform Crime Reports. Such statistical baselines can then be used to measure the effectiveness of the countermeasures recommended by the FACFI as they are being implemented. (Not yet acted upon by the Committee.)

11. *Legislative Loopholes.—*

A. Federal Legislation

The FACFI finds that:

Maintaining and upgrading the integrity of State identification documents, particularly the birth certificate and drivers license, is the key to reducing false identification crimes at both the Federal and State levels.

There are approximately 350 Federal statutes relating to false identification, false applications and related subjects. But Federal laws are ineffective in deterring false identification crimes because:

a. Most identity documents are issued and regulated solely by the states. Federal statutes only come into play when the criminal applies for a federally issued document such as a passport. By this time the criminal has built up such a variety of state-issued documents that false application is difficult to detect and likely to succeed. Indeed, a criminal's false identification may be more persuasive and complete than an honest person's valid identification.

b. The Federal government does not collect and maintain information to verify a person's identity. Only the states have that information. Therefore the Federal government is totally dependent on state information and documents such as the birth certificate and driver's license. And those are often weak links in the identification chain.

c. Because Federal statutes regulate only those documents issued by the Federal government and states regulate only documents which they issue, there remains a substantial enforcement gap between these jurisdictions. This gap permits nationwide counterfeiting and selling of false identification documents.

d. There are loopholes in some of the Federal statutes regulating specific documents, such as the social security card and others.

e. Even where Federal statutes are specific and well drafted, enforcement and prosecution is often given a low priority. The crime usually appears more innocuous than it actually is.

f. Finally, penalties for false statements on applications sometimes require only revocation of licenses. Civil fines are imposed in other instances. In other cases, penalties are sufficient or even excessive.

The FACFI therefore recommends: a. That S. 2131, a bill now pending in the 94th Congress, be enacted. S. 2131 would close most existing loopholes in Federal legislation dealing with false identification. It contains the following provisions: 1. Prohibits *false applications* for Federal documents by prohibiting the knowing use or supplying of false information or falsified documentation when obtaining Federal identification documents;

2. Prohibits the knowing use of the mails or other channels of interstate commerce for *transporting* any false information or documents for the purpose of obtaining State identification documents;

3. Prohibits the unauthorized *making or altering* of any Federal identification documents;

4. Prohibits the unauthorized *making or altering of any State identification document* when there is knowledge that such document will be used to obtain any document by the United States; and prohibits the sale or delivery of any such State identification document;

5. Prohibits using the channels of *interstate commerce or the mails to transmit any false Federal or State identification document* or one intended to be used improperly.

b. That Federal false identification statutes be enforced with renewed vigor by prosecutors; and that judges be made aware of the importance of false identification crimes so that sentences may more accurately reflect the seriousness of these crimes.

B. State Legislation

The FACFI finds that: The primary thrust of state statutes dealing with false identification is prohibitive not preventive. Criminal penalties are invoked upon fraudulent use of a false identity rather than the mere possession of fraudulent identity documents. Laws are totally inoperative until the criminal, in his new identity, commits a crime. By this time it is too late. The criminal has assumed another identity and disappeared;

In most States there is no comprehensive law against establishing a fraudulent identity. Statutes that purport to deal with the problem only deal with parts of it;

State laws governing the issuance of certified copies of birth and death certificates and access to such records do not adequately protect the public's right to privacy because certified copies of birth certificates are freely (though unknowingly) handed to criminals by all states. In some states it is not even illegal to lie on an application for a certified copy of a birth certificate.

The problem is national in scope, but States are powerless to protect any but their own identity documents. States cannot control the manufacture, counterfeiting and criminal use of their own ID documents outside their borders;

The wide variety in document format and authenticating seals encourages the passing of counterfeit State documents;

Laws regulating specific documents, such as the birth certificate, are not comprehensive enough to allow effective enforcement. These laws never make reference to all of the following acts involving false identification:

a. Illegal manufacture.
b. Sale.
c. Possession.
d. Alteration.
e. Transferring.
f. Transporting.
g. Advertising for sale.
h. Obtaining.
i. Receiving.
j. Use or display.
k. Use after expiration, suspension, or revocation.
l. False or misleading statements or use of false documents in an application for such documents.

Without this degree of comprehensiveness, criminals can use and supply others with false identity documents without fear of prosecution.

Many identity documents which can be used for identification purposes or to obtain other documents are not regulated at all. None of the States investigated by the Committee had laws regulating private ID cards and documents not issued by State agencies. These private ID cards can be used to purchase firearms or dangerous drugs that are not traceable to the real purchaser.

Prosecutors place low priorities on prosecution of false ID cases, because of a lack of awareness of the potential seriousness of the crime. Altering a document does not look nearly as serious as a murder or rape case until one realizes that the use of false ID prevents many murder, rape and other cases from being solved.

In most states citizens have the common law right to change their name without any formal legal proceedings. In these states it is more difficult for prosecutors to prove fraudulent intent to violate false ID laws.

The FACFI therefore recommends: a. That States enact Model State Legislation proposed by the Committee, entitled, the Identity Protection Act. This Act provides the following:

Protects the public health and welfare and the right of privacy and security in one's own identity by penalizing the manufacture, alternation, transfer, sale, possession or use of any false identity document or any document obtained by use of false statements or identification in the application process. This act will specifically protect the integrity of the use and possession of birth certificates and driver's licenses. This Act establishes stricter criminal penalties for false identification crimes and requires them to be served consecutively with any other sentence arising out of the same crime.

Finally, the Act prevents fraud by private ID vendors and prohibits spurious documents issued by criminals in other states.

b. That States enact the most recent amendments to Model State Vital Statistics Act which are designed to protect the integrity of the birth certificate issuing system. These amendments also upgrade criminal penalties for false identification crimes.

c. That State educational programs be established to facilitate implementation of the Model Identity Protection Act and the Model State Vital Statistics Act and to assist officials in improved methods of document fraud detection.

12. *Use of Identification Documents for Undercover Purposes.*— The FACFI finds that a study of the means by which Federal, State and local agencies obtain and use undercover documents for law enforcement and intelligence purposes is outside of the charter of the Committee and thus has not been explored; the Committee notes, however, that some have questioned the adequacy of controls on obtaining and using such documents.

The FACFI therefore recommends that: (1) government agencies should not obtain or provide "alias identification" in violation of any local, state, or Federal laws; and (2) recommends that agencies review their laws, regulations and procedures for obtaining such credentials to insure that they are lawfully obtained and that their use is adequately controlled. (Not yet acted upon by the Committee.)

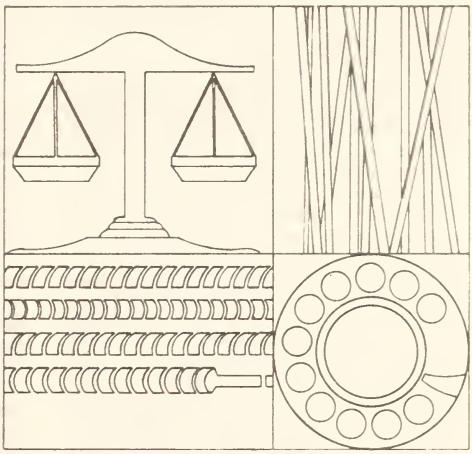
13. *Public Support.—The FACFI finds* it essential to obtain public recognition of the scope and impact of crime committed with the aid of false IDs and to solicit informed support of measures designed to reduce the use of false IDs in the United States.

The FACFI therefore recommends that the Department of Justice and all other concerned organizations undertake a coordinated program of public education with the aim of obtaining a strong public mandate for the measures recommended by the FACFI.

RICHARD L. THORNBURGH,
Assistant Attorney General.

[FR Doc.76-17296 Filed 6-15-76;8:45 am]

U.S. National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. Electronic surveillance. Washington, D.C.: U.S. Govt. Print. Off., 1976: xi-xix.



Electronic Surveillance

REPORT
OF THE
NATIONAL
COMMISSION
FOR THE REVIEW
OF FEDERAL
AND STATE LAWS
RELATING TO
WIRETAPPING AND
ELECTRONIC
SURVEILLANCE

WASHINGTON:
1976

May be cited as
NWC Report

79-064 O - 76 - 31

FOREWORD

The report which follows is the result of two years of work by the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance.

In the course of its two years of work, the Commission held 17 days of hearings, receiving testimony from more than 100 witnesses. In August 1974, 14 experienced prosecutors and investigators conferred for three days in an attempt to determine how, when, and why electronic surveillance can best be used in law enforcement. Commission staff members visited 46 State and 12 Federal law-enforcement jurisdictions to study and report on the manner in which court-authorized and consensual electronic surveillance is being used. Background studies of various aspects of electronic surveillance were prepared by the Commission staff and consultants. (A majority of the Commission determined not to study the use of electronic surveillance in national security cases.)

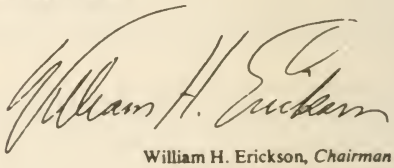
This volume contains the Findings and Recommendations of the Commission, a Summary of the Evidence considered by it, and Minority and Concurring Reports. The testimony taken at our hearings and the reports of the staff and consultants have been published in five separate volumes of supporting materials.

I take this means of commending and thanking those law enforcement officers—both Federal and State—who opened their files for our examination. Their wholehearted cooperation assisted us materially in carrying out our work. Also deserving of our special thanks are the many witnesses, consultants, and advisers who gave us the benefit of their expertise.

The work of the experienced and dedicated Commission staff, under the leadership of Kenneth J. Hodson, our Executive Director, made it possible for us to gather and analyze an impressive amount of relevant evidence about electronic surveillance—court-authorized, consensual, and illegal—thereby enabling us to make a thorough review of the subject.

The objectivity and thoroughness of our study would not have been possible, however, had it not been for the conscientious work of the Commission members, each of whom brought to our work a broad variety of knowledge and experience and a willingness to listen to testimony from witnesses with different backgrounds and experience, and widely varying philosophies. These witnesses were subjected to the most rigorous and critical examination by the Commission members, and I am sure that our record will show that all aspects of the subject of electronic surveillance were exhaustively explored.

The five volumes of supporting materials constitute a record that provides a sound basis for the report which follows.



William H. Erickson, *Chairman*

SUMMARY

BACKGROUND OF THE COMMISSION

Congress established this Commission to study and evaluate the effectiveness of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. 2510–2520), hereinafter Title III, which governs the use of electronic surveillance,* i.e., wiretapping and bugging, in the United States, except in cases involving national security.

When Title III was enacted there were several conflicting views of the form any legislation regulating electronic surveillance should take: at one extreme were those who believed that a total ban on electronic surveillance was necessary for the protection of individual privacy; and at the other extreme were advocates of strong law enforcement who hesitated to limit the use of a technique claimed by many to be a vital tool in fighting crime, particularly organized crime.

Title III was enacted as a compromise of these opposing views. It permitted the use of court-authorized electronic surveillance by law enforcement officers in the investigation of certain enumerated crimes under procedures designed to afford the greatest possible protection to individual privacy. Title III banned completely the use of electronic surveillance by private individuals without the consent of any of the parties to the conversation.

The National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance was created, as part of the compromise, to conduct a comprehensive study and review of the operation of Title III in the first six years after its enactment. In carrying out this Congressional mandate, the Commission concentrated its efforts in three principal areas: Determining (1) whether court-authorized electronic surveillance under the provisions of Title III is an effective tool in law enforcement; (2) whether it adequately minimizes the invasion of the privacy of the individual; and (3) whether Title III is effective in preventing illegal wiretapping and bugging. A majority of the Commission determined that it was not within the scope of its statutory mandate to study the use of electronic surveillance in the national security area.

CONCLUSIONS OF THE COMMISSION

I. Court-Authorized Electronic Surveillance

A. Need for Electronic Surveillance: A majority of the Commission vigorously reaffirmed the finding of Congress in 1968, when it enacted Title III, that electronic surveillance is an indispensable aid to law enforcement in obtaining evidence of crimes committed by organized criminals. It also reaffirmed the Congressional decision that the interception of a wire or oral communication, where none of the parties to the communication consents, should be allowed only when authorized and supervised by a court of competent jurisdiction, and only for the purpose of investigating certain major types of offenses and specific categories of crime.

[A substantial minority of the Commission disagrees with this broad general approval of court-authorized wiretapping. This minority found that court-authorized surveillance had been used successfully in a limited number of major cases, and has resulted in the conviction of only a few upper-echelon crime figures; more frequently, however, court-authorized surveillance has proven to be costly and generally unproductive, has served to discourage the use of other investigative techniques, and, even under the authorization and supervision of a court, has resulted in substantial invasions of individual privacy. This minority recommended that Congress examine the entire range of issues, theoretical as well as procedural, which underlie Title III.]

---

* As used in this summary and in the Commission report, the term *electronic surveillance* generally includes *wiretapping* and *bugging*, although, as indicated in the name of the Commission, the terms *electronic surveillance* and *wiretapping* are sometimes used interchangeably. *Wiretapping* generally refers to the interception (and recording) of a communication transmitted over a wire from a telephone, *without* the consent of any of the participants. *Bugging* generally refers to the interception (and recording) of a communication transmitted orally, *without* the consent of any of the participants. The term *consensual surveillance* refers to the overhearing, and usually the recording, of a wire or oral communication *with* the consent of one of the parties to the conversation.

B. Effectiveness in Certain Crimes: Electronic surveillance was found to be especially effective in investigations of ongoing, conspiratorial criminal activities which involve a high degree of organization, such as gambling, fraud, and dealing in narcotics. The Commission studied a number of cases in which imaginative and sophisticated use of court-authorized electronic surveillance established proof of serious offenses involving well-organized criminal hierarchies, after traditional investigative means had been used without success.

Some members of the Commission felt that the Federal emphasis on use of electronic surveillance in gambling operations has distracted attention from its great potential for use in other types of investigations. Federal officials defended their use of court-authorized electronic surveillance in gambling cases on the grounds that gambling provides the financing for many of the activities of organized crime, and the gambling networks provide an insight into the structure of organized crime. To a certain extent, also, the Federal concentration of electronic surveillance in gambling investigations has resulted from jurisdictional limitations. Fencing, murder, and arson, for example, are typically local crimes which Federal agents have no power to investigate. The fact that crime control is primarily a local rather than a Federal concern is reflected in the statistics on the number of wiretaps and bugs installed in the first seven years of the operation of Title III: of the total of 4138 devices installed, 3193 were installed by State officials and 945 by Federal officials.

A majority of the Commission concluded that electronic surveillance could be used with significant sucess in the investigation of Federal crimes not now included in the enumerated crimes of Section 2516 of Title III, such as customs offenses, interstate shipment of firearms, and interstate fencing of stolen goods.

C. Effectiveness of Certain Procedures

Personnel: Electronic surveillance was found to be most effective when conducted by an experienced prosecutor, backed up by an adequate and trained staff of assistant prosecutors, working closely with experienced investigators. A strong case can be made for the "strike force" approach to investigations under Title III, with the close cooperation between attorneys and investigators demonstrated by the Federal Strike Forces. Such an approach is of even more value in Title III investigations than in ordinary criminal investigations because of the complex legal procedures involved in Title III surveillances. The Commission observed that prosecutors and investigators have in fact been working in increasingly close cooperation as they have gained experience with Title III.

Training: The Commission found that on the whole there was insufficient training of both Federal and local law enforcement personnel in the techniques of electronic surveillance, that is, training which emphasizes how, when, and why to use this important investigative tool. Training of both investigators and attorneys is now generally on an apprentice system, which has major flaws: what is taught is generally limited by the electronic surveillance experience within the jurisdiction; the training is on a case-by-case basis which may lead to gaps in the information taught; and perhaps most importantly, this method of training does not always lead to imaginative or innovative use of electronic surveillance.

The Commission has recommended that the Federal government provide for training of Federal and local law enforcement personnel in the techniques and laws governing electronic surveillance.

Application procedures: The Commission found that the procedures developed by the Department of Justice for the review of wiretap applications reflect a commendable concern for adhering to the requirements of Title III. The major disadvantage of such elaborate procedures was the time required to process the applications under circumstances where time might be a critical factor.

A majority of the Commission therefore recommended that the Department of Justice consider streamlining or decentralizing its application review procedures, perhaps by greater delegation of decisionmaking responsibility to experienced United States Attorneys or Federal Strike Force Chiefs. It was also recommended that Congress amend Title III to permit the Attorney General to designate, by name, any U.S. Attorney or Strike Force Chief to authorize wiretap applications, provided that a copy of the application is filed with the Attorney General for concurrent review.

[A substantial minority of the Commission dissented from this recommendation, fearing that such a procedure might undermine the protections offered by the clearly traceable lines of responsibility provided for in the 1968 law. The suggestion was made that a more flexible approval mechanism might be adopted which would allow the Attorney General to approve applications by telex or telephone rather than in writing in certain cases where time is of critical importance.]

In contrast to Federal procedures, state procedures

generally reflected too little centralization. If a local jurisdiction is unable to assign adequate personnel to a tap, or is unable to follow a case across county lines, the electronic surveillance effort may be counterproductive. The Commission has recommended that states provide for state-wide oversight and concentration of resources for the use of electronic surveillance in law enforcement.

Recordkeeping: Recordkeeping by prosecutors of the results of court-authorized electronic surveillance was found to be inadequate. Under Section 2519 of Title III, judges and prosecutors are required to report certain information about each application, such as the number of convictions resulting from the interception, to the Administrative Office of the United States Courts. This information, while not essential to the execution of the individual wiretap, is basic to any review of the effectiveness of Title III. The Commission staff found that few prosecutors actually keep records which trace the course of their wiretaps from the inception of the wiretap to the final disposition by dismissal, acquittal, or conviction and sentence.

The Commission recommended that prosecutors keep sufficient records to permit ready evaluation of the effectiveness of their use of electronic surveillance, noting that perhaps the Department of Justice would be better equipped to collect and analyze prosecutors' reports than the Administrative Office.

D. Federal-State Cooperation: The Commission found that there has been insufficient Federal-State cooperation in wiretap investigations. Cooperation is a two-way street and it is critically important in Federal or state investigations of any organized, conspiratorial, ongoing criminal activity of significant size. It is particularly important in those investigations which may require the use of electronic surveillance by either State or Federal authorities, or both.

The problem of cooperation and exchange of information is made more difficult when state law not only forbids court-authorized wiretapping but doesn't allow the use of legally obtained Federal evidence in state courts, as is now the case in California and Pennsylvania.

The Commission recommended that states which have a significant rate of organized-crime-type offenses should enact wiretap legislation consistent with Title III. (This type of legislation has already been enacted by 21 states and the District of Columbia. The States of Pennsylvania and Washington, although theoretically permitting court-authorized surveillance, are not included in this number, as their laws are so restrictive as to prohibit any effective type of electronic surveillance, even with the authorization of a court.) There was a further recommendation that Federal-State cooperation be encouraged, where necessary, by State laws making Federal wiretap evidence admissible in state courts.

[A substantial minority of the Commission feels that it is inappropriate for this Commission to comment on state laws, and does not concur in this recommendation.]

E. Telephone Company Cooperation: The Commission found that telephone companies have generally cooperated with law enforcement officials in providing information necessary for the installation of wiretapping devices and in providing "leased lines" (lines which permit the police to monitor the wiretap from a central location). The Commission did find, however, that in a few instances telephone companies have refused to aid police who had court authorization to conduct a wiretap. Also, in several states telephone companies have refused to assist the police by providing leased lines, thereby requiring the officers to establish plants in surroundings which are sometimes dangerous, and which may jeopardize the security of the surveillance.

The Commission has recommended that state wiretap statutes should include a provision, similar to the one which was added to Section 2518(4) of Title III in 1970, directing telephone companies to furnish all necessary information and assistance to permit accomplishment of a court-authorized wiretap unobtrusively and with minimum interference.

II. Consensual Surveillance

Electronic surveillance carried out with the consent of one of the parties to the conversation is not a "search" for criminal conversations within the meaning of the Fourth Amendment and therefore does not require court authorization. Its basic use is to corroborate conversations, thereby improving the accuracy of evidence for use in court.

The Commission found that consensual electronic surveillance by law enforcement is especially useful in the investigation of certain crimes, particularly official corruption, extortion, and loansharking. It also serves to protect the consenting party to the conversation. A majority of the Commission recommended that Title III should not be amended to require court-authorization for consensual surveillance, as has been suggested by some.

However, a recent sharp increase in the number of consensual surveillances by Federal law enforcement

officers has been noticed, accompanied by a slight decrease in the number of court-authorized surveillances. The Commission recommended that Congress examine this trend to determine whether any legislative safeguards should be provided for consensual surveillance.

It was also found that in some cases consensual surveillance equipment has been subject to misuse and theft. The Commission recommended that careful administrative controls, such as check-in/check-out records and strict inventories, be instituted to prevent such abuses.

III. Protection of Privacy

A. Effectiveness: The Commission concluded that the procedural requirements of Title III have effectively minimized the invasion of individual privacy in electronic surveillance investigations by law enforcement officers. When properly implemented, Title III procedures have served to protect the privacy not only of innocent individuals but also of the persons who are the subject of the investigation. Some modifications recommended by the Commission, however, could serve to enhance the protections of Title III.

B. Conduct of Law Enforcement Officers: There were no cases, among the many studied by the Commission, in which law enforcement authorities sought a Title III court order for an apparently corrupt purpose. Furthermore, once a Title III investigation is underway, the many record-keeping requirements and procedural controls of the statute greatly inhibit misuse of the intercept or the information obtained. For example, the Commission staff was able to measure, through review of the records, the extent of minimization efforts in the wiretap cases it studied. Investigating officials know of these record-keeping requirements and know that a disregard of them may result in invalidation of the surveillance evidence.

The Commission found that there have been cases, especially in the early days of Title III, in which law enforcement authorities failed to adhere to the procedural requirements. This was due, in some cases, to familiarity with the pre-Title III practice of using wiretaps to gain intelligence about general criminal activity rather than to gather evidence for the trial of a specific offense. The Commission found that continuing experience with Title III resulted in a universally consistent improvement in adhering to procedural requirements such as minimization.

C. Procedural Protections

Exclusionary rule: In addition to providing civil and criminal penalties for violations of its provisions, Title III expressly forbids the use in court of electronic surveillance evidence obtained in violation of its terms. The Commission found that this exclusionary rule has been effective in causing investigators, prosecutors, and judges to adhere to the procedural requirements of Title III. The criticism levelled at the exclusionary rule in searches generally—that it does not prevent unlawful searches because the police officers conducting the search are not conscious of the prosecutor's later problems at trial—does not necessarily apply to Title III investigations because the prosecutor is involved in an electronic surveillance investigation from the outset. The Commission therefore recommended that the Title III exclusionary rule be retained, regardless of the fate of such a rule with regard to other law enforcement searches.

Appeal: Because wiretap evidence is so strong, the defendant has little choice except to plead guilty if his motion to suppress wiretap evidence is denied. Under current Federal practice, however, a plea of guilty precludes consideration on appeal of the denial of such a motion. The defendant can preserve his appeal on the suppression ruling only by pleading not guilty and going to trial. The Commission has recommended that current Federal practice be amended to permit an appeal after a guilty plea, in order to obviate the need for a full trial on the merits simply to preserve the right to have the suppression ruling considered on appeal.

Minimization: Title III requires the minimization of conversations not subject to the court order. This requirement presents prosecutors with a dilemma: Too much minimizing may lead to a charge by a defendant that exculpatory evidence was not included in the recording; too little minimizing, on the other hand, may invade privacy in a way that invites suppression. The Commission found that the term "minimization" was not susceptible to statutory definition; it must be determined on a case-by-case basis by the courts. The Commission adopted the language used by several Federal courts that if, in light of all the facts and circumstances of a case, the agents have shown a high regard for the right of privacy and have done what they reasonably could to avoid unnecessary intrusion, the minimization requirement will be satisfied.

Alternative investigative means: The Title III requirement that a wiretap application include a "full and complete" statement whether other investigative procedures have been tried and failed, or why they appear to be unlikely to succeed if tried, or to be too dangerous to try, has often been met by standardized language. The use of standardized language is often

inevitable because the investigative methods themselves tend to be standardized, especially in crimes such as gambling.

The Commission found, however, that standardized language was sometimes used in situations where more particularized information could have been offered. As the exhaustion of alternative means is a vital prerequisite to the use of court-authorized surveillance, the Commission has recommended that Section 2518 be amended to require consideration of the particular facts of a case, insofar as practicable, in the discussion of investigative techniques.

D. Additional Safeguards

Extensions: A majority of the Commission found that most court-authorized surveillances have not been unduly long, although a few have been unnecessarily extended. Of the cases surveyed by the Commission staff, only one Federal wiretap out of 547 ran longer than 60 days. But 102 out of 762 state taps lasted more than 60 days. Because different offenses require different periods of time, and because unduly lengthy surveillances can be prevented by requiring the extension application to show additional facts justifying the requested extension, the majority concluded that it would be unwise to shorten the period of the initial tap or to place an arbitrary limit on the length and number of extensions.

[A substantial minority of the Commission felt that the interests of privacy would be better served if the initial authorized period for electronic surveillance orders were reduced from the present 30-day period to 15 days, and the current provision permitting unlimited 30-day extensions were amended to allow only one 15-day extension.]

The majority recommended that Section 2518 be amended to require a showing of some special reason for extending the surveillance, such as the receipt of new information concerning additional offenses or offenders, or information indicating that the subjects will communicate about the offense during the extension.

Notice: Under Section 2518(8)(d) of Title III, it is left to the discretion of the judge to determine what persons, other than those named in the order, should receive notification of having been heard on a wiretap. The Commission found that the judge is dependent on the prosecutor to give him the names of persons who have been intercepted.

A majority of the Commission concluded that Section 2518 should be amended to provide that in the event that a surveillance is ultimately found to have been *unlawful*, all persons who have been identified should be notified. Notification in such cases would give all parties necessary information to permit them to sue for malicious conduct and to challenge any subsequent prosecutions which might have been tainted by the illegal surveillance. Following a legal interception, the persons to be notified should include, as a minimum, those intercepted persons who are indicted or are expected to be indicted, or who are expected to be called as witnesses, as well as those who are the subject of the surveillance order.

[A minority of the Commission would require notification of all intercepted persons who are identified—even though clearly innocent—if their names are entered into any type of surveillance file or index.]

E. Emergency Provision: The Commission found that law enforcement officials have been hesitant to use the Title III emergency provision, which permits electronic surveillance without a court order in an emergency situation involving national security or organized crime, provided that court authorization is sought within 48 hours of the beginning of the intercept. A majority of the Commission found that emergency surveillance might be useful in offenses involving death or serious bodily injury, even though there is no threat to national security and no involvement of organized crime. The majority did recommend, however, that the provision be amended to require oral notification of a judge prior to installation of the emergency tap.

[A minority of the Commission felt that in view of the doubtful constitutionality of the provision and its potential for abuse, it should be abolished.]

F. Bugs and Other Devices

Bugs: In its investigation, the Commission found that some law enforcement officers doubt whether they have authority to use a bug in situations where a surreptitious entry is required to install the device and the order does not include specific authorization for the entry.

Some members of the Commission felt that eavesdropping devices are so intrusive on personal privacy that their use by law enforcement should be prohibited, except perhaps in national security cases. The majority recognized, however, that they are indispensable to law enforcement in certain situations, and, in many instances, are less intrusive than wiretaps. Because of the reluctance of law enforcement officials to use a bug if a surreptitious entry is required, it was recommended that court orders should include express authorization to enter upon premises,

if necessary to install the devices.

Other devices: Ambiguity exists with respect to certain other devices which are essential to law enforcement, but which are not now included under Title III. The Commission recommended that the law with regard to devices such as the "bumper beeper" (a device which electronically signals the location of an object, such as an automobile) and the "pen register" (a device which records the telephone number dialed on an outgoing call) be clarified, either by amending Title III to include them, or by revising state and Federal rules of criminal procedure.

IV. Illegal Surveillance

A. Incidence: The average citizen's fears that he might be the victim of electronic surveillance are mainly unjustified. Over two billion telephone calls were placed in the United States in 1974 alone, yet between January 1, 1967, and December 30, 1974, the American Telephone and Telegraph Company reported finding only 1555 unauthorized eavesdropping devices on its lines. The large majority of illegal eavesdropping involves marital or family relations. Far down the scale are industrial, political, and police spying.

Although it is impossible to determine the exact amount of illegal surveillance, it is generally acknowledged that Title III has reduced the incidence of such illegal interceptions through its controls on the manufacture, sale, and advertising of surreptitious devices and its criminal sanctions for their use. The open and prolific advertising of wiretapping devices, for example, has been substantially—though not entirely—eliminated. There was a strong feeling that more can and should be done to enforce the criminal sanctions of Title III.

The Commission found instances of illegal electronic surveillance by local law enforcement officers acting without court authorization, some of which was carried on to aid law enforcement and some of which was for the purpose of financial gain. Subject to the proviso that the Commission studied no electronic surveillance conducted under the label of "national security," the Commission found no confirmed instances of illegal surveillances by Federal authorities. There were allegations, however, that Federal authorities received information from State police which they reasonably should have known was derived from illegal wiretapping. This also would be illegal under the provisions of Title III.

The Commission found that firmer control over the dissemination of electronic surveillance equipment by the agencies which possess it could help prevent illegal surveillance by law enforcement officials. To that end, the Commission recommended that only those officers whose duties make it necessary for them to use or possess electronic eavesdropping devices should be exempted from the provisions of Title III banning possession of such devices.

B. Enforcement: Enforcement of the criminal provisions of Title III has been difficult for a number of reasons, such as (1) understaffing in the enforcement section of the Department of Justice, (2) judicial and jury reluctance to condemn violators to the severe penalties of Title III or to convict individuals who claim to be motivated by a wish to uncover wrongdoing, and (3) the reluctance of victims to testify, particularly as to marital or family relations eavesdropping.

The Commission made a number of recommendations to improve this situation. It suggested affirmative enforcement programs by the Department of Justice and state law enforcement agencies for the detection and prosecution of professional eavesdroppers. The Commission also recommended strict enforcement of the prohibition on manufacture and sale of surveillance devices, especially those sold in the guise of "baby monitors" and "burglar alarms."

The Commission recommended that Congress amend Title III to include misdemeanor penalties to encourage conviction by ambivalent juries, and a substantial minority of the Commission recommended a significant increase in the amount of civil damages available under the statute to encourage individual lawsuits against violators. Further, it was recommended that Title III be amended to explicitly provide for the disclosure of illegal interceptions in prosecutions of illegal wiretappers—an area of the statute that is found by some courts to be ambiguous—while allowing the judge to retain discretion to deny use of the evidence where its relevance is outweighed by undue loss of privacy to the victim.

C. Manufacturers and Distributors: Title III's prohibition against the manufacture, sale, and advertising of devices "primarily useful for . . . the surreptitious interception of wire or oral communications" has resulted in a notable drop in the open manufacture and marketing of such devices. However, the manufacturers who furnish devices to law enforcement authorities for use under Title III are largely unregulated. The Commission has recommended that State and local legislative bodies undertake to regulate such activities, perhaps through a system of licensing.

Manufacturers testified before the Commission that the vague "primarily useful" language of the statute has put them in the position of not knowing if and when they are violating Title III. The Commission responded by recommending that Congress authorize the Department of Justice to issue regulations defining specifically proscribed devices and providing rules for maintaining inventory control.

D. Countermeasure Services: The Commission found that individuals and firms holding themselves out as countersurveillance experts are basically unregulated, and the public is without standards for evaluating their services or the need for such services. The Commission heard an abundance of evidence to the effect that the fears of the public were being inflamed by the exaggerated claims of disreputable countermeasure firms trying to drum up extra business. A related problem is the absence of any requirement that persons claiming to find such devices turn them over to law enforcement for investigation.

The Commission recommended that Congress and the states provide for the regulation of those offering countersurveillance services, to include a requirement that they report any devices which are found.

V. Further Review of Title III

The Commission recommended that a comprehensive study and review of the operation of the provisions of Title III be made periodically.

VI. Other Areas Involving the Invasion of Privacy in Which Further Study is Recommended

The Commission heard evidence concerning encroachments on privacy in the private sector, such as (1) abuse of private consensual recording, (2) computer data interception, (3) monitoring of employees by supervisors in the interest of providing better service to telephone customers, and (4) the investigation of toll frauds by telephone companies. It recommended that Congress study these areas of privacy invasion to determine whether legislative or regulatory safeguards are necessary and desirable.

U.S. Privacy Protection Study Commission. Federal tax return confidentiality. Washington, D.C.: U.S. Govt. Print. Off., 1976: 1-8.

FEDERAL TAX RETURN CONFIDENTIALITY

REPORT OF THE

Privacy Protection Study Commission

2120 L Street N.W.
Washington, D.C. 20506

June 1976

PRIVACY PROTECTION STUDY COMMISSION
2120 L STREET, N.W.
WASHINGTON, D.C. 20506

June 9, 1976

President Gerald R. Ford
The White House
Washington, D.C.

Dear Mr. President:

On behalf of the Privacy Protection Study Commission, I hereby transmit to you the Commission's summary report and recommendations on Federal tax return confidentiality.

The Commission was created by Public Law 93-579, the Privacy Act of 1974. Section 5(c)(2)(B)(ii) of the Act requires the Commission to report to the President and the Congress on:

> *whether the Internal Revenue Service should be prohibited from transferring individually identifiable data to other agencies and to agencies of State governments.*

The Commission assigned high priority to a review of the Internal Revenue Service's disclosure policies because of the important public policy issues involved. Accordingly, I am transmitting our recommendations to you with a summary of the rationale on which they are based. A more extensive Commission report on Federal tax return confidentiality will be issued at a later date.

The Commission is pleased to transmit this, its first report, to you. We are keenly aware of your longstanding interest in the protection of personal privacy and believe that our work on the confidentiality of tax records represents a constructive contribution to the debate on this complex matter.

Sincerely,

/s/ David F. Linowes

David F. Linowes
Chairman

RECOMMENDATIONS
OF THE
PRIVACY PROTECTION STUDY COMMISSION
ON
FEDERAL TAX RETURN CONFIDENTIALITY

****

GENERAL RECOMMENDATIONS

The Privacy Protection Study Commission recommends:

(1) that no disclosure of individually identifiable data by the Internal Revenue Service be permitted without the prior, written consent of the individual to whom it pertains, except when such disclosure has been specifically authorized by Federal statute;

(2) that the Congress provide by statute that the Commissioner of Internal Revenue may disclose to a Federal or State agency that is specifically authorized by statute to obtain individually identifiable information from the Service only such information as that agency needs to accomplish the purpose for which such disclosure is made and, further, that the Commissioner of Internal Revenue adopt administrative procedures that permit public scrutiny of the Service's compliance with this statutory requirement;

(3) that the Congress specify in each statutory authorization for disclosure the categories of information that may be disclosed and the purpose for which the information may be used; and

(4) that a recipient of individually identifiable tax information from the Service be prohibited from redisclosing such information without the consent of the individual to whom it pertains, unless specific authorization for such redisclosure has been expressly provided by Federal statute.

SPECIFIC RECOMMENDATIONS

Within the framework of the foregoing General Recommendations, the Privacy Protection Study Commission further recommends:

Federal Tax Administration

(1) that the Congress permit the Internal Revenue Service to disclose individually identifiable data to the Department of Justice for use in investigations and prosecutions of violations of tax laws, provided that the information pertains to a party to the actual or anticipated litigation;

(2) that the Congress permit the IRS to disclose to the Department of Justice information about an individual who is not being investigated or prosecuted for a violation of the tax laws provided that the information disclosed is relevant to issues in an actual or anticipated tax litigation. In such cases, however, information about an individual should be considered relevant only if the treatment of an item on the return of a party to an actual or anticipated tax litigation, or the liability of such a person for any tax, penalty, or interest, may be determined by reference to it;

(3) that the Congress permit the Internal Revenue Service to disclose to the Social Security Administration (SSA):

(a) employers' quarterly tax returns and income tax returns of self-employed individuals, for the purpose of administering Title II of the Social Security Act; and

(b) registration statements that pension plan administrators are required to file with the Internal Revenue Service for the purpose of carrying out SSA's responsibilities under the Employee Retirement and Income Security Act (ERISA).

(4) that the Congress permit the Social Security Administration to obtain name and address information

from the IRS for the purpose of notifying individuals of their eligibility for Title II benefits;

(5) that the Congress permit the Internal Revenue Service to disclose tax returns of employers subject to the Railroad Retirement Act to the Railroad Retirement Board for use in verifying compensation credited to an individual's account by the Board;

State Tax Administration

(6) that the Congress permit the Internal Revenue Service to disclose individually identifiable IRS data to a State agency responsible for tax administration or enforcement for the sole purpose of determining, validating, or enforcing a taxpayer's liability under a general revenue law of the State, provided that--

(a) the disclosure of tax information to State agencies for such purposes is limited to the information on a Federal income, estate, or gift tax return (Forms 1040, 1040A, 706, and 709) and accompanying schedules, and summary information regarding adjustments to such returns, that is necessary to determine taxpayer liability under a general revenue law of the State;

(b) requests for the disclosure of individually identifiable IRS data are made in writing by the principal tax official(s) of a State;

(c) a State which seeks to obtain individually identifiable IRS data must have enacted a statute with penalties substantially similar to those of Section 7213 of the Internal Revenue Code, prohibiting the disclosure for purposes other than State tax administration of Federal tax information obtained from the Internal Revenue Service, as well as information supplied by the State taxpayer that is a copy of or copied from his Federal tax return;

(d) a State be permitted to continue to receive Federal tax information for a period of two years after the adoption of the foregoing recommendations by the Congress pending the enactment of the necessary statute by its legislature. If, however, the necessary State legislation

has not been enacted by the end of that two-year period, the Commission recommends that the Service be required to discontinue the disclosure of information to the State until the necessary statute is enacted;

(e) a State that receives individually identifiable data from the IRS is required to institute reasonable physical, technical, and administrative safeguards satisfactory to the IRS to avoid the use or disclosure of such information for purposes other than State tax administration;

(f) the Internal Revenue Service is required to review the administrative, technical, and physical safeguards established by each State pursuant to the foregoing recommendation and the Commissioner of Internal Revenue is empowered to suspend temporarily a State's access to Federal tax information if an unauthorized disclosure is made, or if the safeguard procedures in force are determined to be inadequate; and

(g) a procedure is established to permit a State to appeal a decision by the Service to suspend its access to Federal tax information.

Local Tax Administration

(7) that the Congress permit a State taxing authority to use for purposes of local tax administration any Federal tax information it could obtain for State tax administration, provided, however, that such information is not disclosed to the locality;

(8) that the Congress permit the Internal Revenue Service to disclose to a local taxing authority the name, address, and type of return filed of all Federal taxpayers in that locality, provided, however, that the information is supplied directly to the locality by the Internal Revenue Service and that the locality has enacted, and is enforcing, an ordinance prohibiting the use of such information for purposes other than local tax administration;

(9) that the Congress permit the Internal Revenue Service to disclose the Social Security numbers of Federal taxpayers in a locality if the locality had in force before January 1, 1975, a law allowing it to demand the Social Security number directly from such taxpayers for local tax purposes;

Statistical Purposes

(10) that the Congress permit the Internal Revenue Service to disclose to the Bureau of the Census information from individual income tax returns (Forms 1040 and 1040A), provided that no more information is disclosed to the Bureau than is necessary for its purposes;

Prospective Federal Appointees

(11) that the Congress not permit the Service to disclose information about prospective Federal appointees without the consent of the individual to whom the information pertains;

Parent Locator Service

(12) that if the Congress permits the Federal Parent Locator Service to continue to have access to information maintained by the Internal Revenue Service, such access be limited to instances in which the residence and place of employment information sought may serve to locate an individual against whom there is an outstanding court order for child support, the financial requirements of which are not being met; there be a strict prohibition on the redisclosure of taxpayer identity information by any Federal or State agency recipient entitled to receive it from the Parent Locator Service; and the penalties of Section 7213 of the Internal Revenue Code for unauthorized disclosure of tax information be made applicable to such recipients;

Taxpayer Identification Information

(13) that no disclosures of taxpayer identification information by the IRS be authorized save those that would be permissible pursuant to the specific disclosure authorizations recommended in other sections of this report;

Non-Tax Law Enforcement

(14) that the Congress prohibit the Commissioner of Internal Revenue from disclosing individually identifiable information about a taxpayer to another Federal agency for non-tax law enforcement purposes unless the Commissioner is in receipt of a court order issued pursuant to the following 6-part procedure:

(a) a Federal agency with civil or criminal law enforcement authority shall file an application through the United States Department of Justice, or directly if it is authorized to do so, with an appropriate United States District Court for an order granting access to information the Internal Revenue Service maintains on an individual. In its application, the agency shall have reasonably described the information it seeks;

(b) the applicant agency shall serve the taxpayer to whom the requested information pertains in the same manner as it would serve an adversary party in initiating litigation. The taxpayer shall have 20 days following service of process to respond;

(c) the U.S. District Court shall have jurisdiction to order the IRS Commissioner to disclose the information sought where the applicant agency has maintained its burden to prove:

(i) probable cause to believe that a violation of civil or criminal law has occurred;

(ii) probable cause to believe that the tax information requested from the IRS provides probative evidence that the violation of civil or criminal law has occurred; and

(iii) there would be no legal impediment to the applicant agency acquiring the information sought directly from the taxpayer;

(d) the taxpayer shall be permitted to participate fully in all proceedings pursuant to the application to the court. The District Court judge may require that the information sought be submitted by the Internal Revenue Service for his review in camera. If service of the taxpayer cannot be reasonably effected, the application may proceed at the discretion of the court without participation by the taxpayer;

(e) if the court determines that the applicant agency is not entitled to obtain an order

79-064 O - 76 - 32

substantially requiring the Commissioner of Internal Revenue to produce the requested information, the court may order that the applicant agency reimburse the taxpayer for litigation costs, including reasonable attorneys' fees incurred in connection with the application proceedings; and

(f) the order issued by the District Court, directing the Commissioner of Internal Revenue to deliver the information sought, shall be considered a final order of the District Court and subject to appropriate review;

(15) that the Congress not permit the disclosure of any tax information about a prospective juror for use in jury selection,

Federal Agency Safeguards

(16) that the Congress provide that the Internal Revenue Service may require Federal agencies that obtain individually identifiable data from the IRS to institute reasonable administrative, technical, and physical safeguards satisfactory to the Service to avoid the unauthorized use or disclosure of such information. The Commission recommends further that if the President and Committees of Congress obtain individually identifiable data from the IRS they, too, be required to institute reasonable administrative, technical, and physical safeguards satisfactory to the IRS to avoid the unauthorized disclosure of that information;

Penalties for Unauthorized Disclosure

(17) that the Congress amend Section 7213 of the Internal Revenue Code to increase the maximum fine from $1,000 to $5,000, and to make Section 7213 apply to former employees of Federal, State, and local government agencies, private contractors, and any other individual authorized to obtain Federal tax information;

Use of the Social Security Number by State Taxing Authorities

(18) that the Congress provide by statute that a State taxing authority may require a State taxpayer to

disclose his SSN to the State taxing authority, provided, however, that the statute prohibits the use or disclosure of the SSN for purposes other than State tax administration, and that penalties comparable to those in Section 7213 of the Internal Revenue Code be applied to the unauthorized disclosure of the SSN by an officer or employee of the State taxing authority.

C. Courts

REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications

To the Senate and House of Representatives of the United States of America in Congress Assembled:

This report is submitted in accordance with the provisions of Title 18, United States Code §2519(3) which require that in April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire or oral communications. Included here are the number of orders and extensions granted or denied during 1975, together with a summary and analysis of the data required by law to be filed with the Administrative Office of the United States Courts by federal and state judges and by federal and state prosecuting officials.

This is the eighth report submitted under the Wiretapping and Electronic Surveillance provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which was approved on June 18, 1968 (82 Stat. 218). This report summarizes the period from January 1, 1975 to December 31, 1975. The first report, submitted to the Congress on April 30, 1969, covered the period June 20, 1968 to December 31, 1968. Subsequent reports summarized the interception of communications occurring during calendar years 1969 through 1974.

I. Reporting Requirements of the Statute

The law requires every state and federal judge to file a written report with the Director of the Administrative Office of the United States Courts on each application made to him in accordance with the provisions of Title 18, U.S.C. §2518, for an order authorizing the interception of a wire or oral communication. The report is to be furnished within 30 days "after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order..." and must contain certain detailed information including the name of the applicant, the offense specified in the application, and the duration of the authorized intercept.

Prosecuting officials who have applied for intercept orders are required to file reports on these applications in January covering the previous calendar year. These reports contain information relative to the cost of the intercepts and the results of the intercepts in terms of arrests, trials, convictions and the number of motions to suppress the use of the intercepts.

No information is to be submitted by either the judge or the prosecutor concerning the names, addresses, or telephone numbers of the persons under investigation.

This report tabulates the number of applications for interception authorized by judges as well as the number of applications where interception devices were installed, as reported by prosecuting officials. There are no statistics available on the actual number of devices installed for each application.

II. Regulations

Regulations, including reporting forms, were first promulgated by the Director of the Administrative Office of the United States Courts in November 1968. Each year copies of these regulations are sent to every prosecuting official who made an application during the year, as disclosed from reports filed by judges. The letter of transmittal, the regulations, and a copy of the federal wiretapping statute may be obtained by writing to the Director of the Administrative Office of the United States Courts, Supreme Court Building, Washington, D.C. 20544.

Prosecutors who filed reports in the past years also are requested to provide supplementary reports on additional activities in the current reporting period such as costs, arrests, trials, motions to suppress and convictions which occurred as a result of intercepts authorized in previous years.

The statute requires that orders by state judges approving applications authorizing communication intercepts by state officials may be made only by judges of courts of competent jurisdiction and that applications may be made only by a prosecuting attorney, "if such attorney is authorized, by a statute of that State to make application to a State court judge of competent jurisdiction". The twenty-four jurisdictions which had laws authorizing courts to issue orders permitting wiretapping and electronic surveillance did not change from 1974. Eighteen of these jurisdictions reported use of wiretap statutes in 1975. (Table 1)

Table 1

Jurisdictions with Statutes Authorizing
the Interception of Wire or Oral Communications
Effective During the Period January 1, 1975 to December 31, 1975

State	Statutory Citation*	Reported Use of Wiretap in 1975
Federal.....	18:2510 - 2520	Yes
Arizona.....	13:1051 - 13:1059	Yes
Colorado.....	40-4-26 - 40-4-33	No
Connecticut.....	Public Act No. 68	Yes
Delaware.....	11:XLII.757	Yes
District of Columbia.....	23:541 - 556	Yes
Florida.....	934.01 - 934.10	Yes
Georgia.....	26-3001 - 26-3010	Yes
Kansas.....	22-2513	No
Maryland.....	35-92 - 35-99	Yes
Massachusetts....	272-99	Yes
Minnesota.....	626A.01 - 626A.23	Yes
Nebraska.....	86-701 - 86-707	Yes
Nevada.....	179.515(1)	No
New Hampshire....	570-A:1 - 570-A:11	Yes
New Jersey.....	2A:156A-1 - A:156A-26	Yes
New Mexico.....	40A-12 - 1.1 - 10	Yes
New York.....	813-J - 813-M; 814 - 825	Yes
Oregon.....	133.723,725,727	No
Rhode Island.....	12-5.1-1 - 12-5.1-16	Yes
South Dakota.....	23-13A-1 - 23-13A-11	No
Virginia.....	19.1-89.1	Yes
Washington.....	9.73.040 - 9.73.080	No
Wisconsin.....	968.27 - 968.33	Yes

*Excludes jurisdictions which enacted legislation in 1976.

III. Summary of Reports by Judges

The name of the judge which appears in the appendix is the judge responsible for the original authorization and, in most cases, the extension. The data reported for calendar year 1975 include only those orders for which interceptions were concluded in 1975.

During calendar year 1975, 704 applications for orders to intercept wire or oral communications were made to state and federal judges. Three of these applications were denied by state judges one each in Connecticut, Maryland, and New York. Of the 701 applications granted, 108 were granted by federal judges and 593 were granted by state judges. There were 192 orders authorized by state judges in New York in 1975 compared to 305 in 1974, a decline of 37%. In New Jersey, state judges signed 196 orders which accounted for 33% of all state orders signed. Intercepts authorized and approved in the states of Florida, Maryland, New Jersey, and New York represented 84% of all wiretap authorizations during 1975.

There was a four percent decrease in the total number of wiretap orders authorized, 728 in 1974 compared to 701 in 1975. Federal orders declined by 11 percent from 121 in 1974 to 108 in 1975 and state authorizations decreased by two percent from 607 in 1974 to 593 in 1975.

Table 2 summarizes the number of intercept orders authorized by each reporting jurisdiction, the number of intercept orders reported as being amended, the number of extensions granted, and the average length of the original authorizations and extensions. Table 2 also reflects the total number of days during which intercepts were reported in actual use and the type of location where the interception of communication occurred.

A. Grants, Denials, and Authorized Length of Intercepts:

Authorized length of time for the 701 applications granted for the interception of wire or oral communications varied from one-fourth of a day to 360 days (which included 11 extensions). The United States Department of Justice reported two emergency intercept authorizations granted in the Southern District of Ohio and the Eastern District of Michigan. The actual number of days in operation for these emergency intercepts was one and two days, respectively. The average length of original authorizations was 22 days, compared to 23 days in 1974 and 24 days in 1973. The total number of days in actual operation as reported by prosecuting officials for those orders where conversations were intercepted varied from one-fourth day to 230 days. Twenty original intercept orders were reported as amended. The reported amendments provided for adding or changing the telephone line or the persons to be monitored or the offenses under investigation.

B. Offenses:

The offenses specified in the applications for court orders covered a wide range. Many applications specified more than one crime under investigation. Table 3 presents a breakdown of generally the most serious offense named in the applications. There were 408 authorizations, comprising 58 percent of the total, where gambling was the most serious offense. In 178 authorizations, drug offenses were under investigation. Sixteen applications specified homicide or assault as the major offense.

In the reports submitted by the judges and prosecutors where the offense specified was related to violations of drug laws, the offense appears in this report as narcotics.

C. Type of Location:

The locations of authorized interceptions of wire or oral communications included 264 single family dwellings, 191 apartments, 39 multiple dwellings, 138 business locations, and 45 various combinations of business and living quarters. In 24 authorizations the place of interception was another type of location such as a pay public telephone, an automobile, or a social club.

IV. Reports by Prosecuting Officials

The reports filed by prosecuting officials were generally complete. Where a report was incomplete, special requests were made for the missing information. In the appendix tables, the phrase "no prosecutor report" indicates that the prosecutor failed to submit the required report. In all instances the prosecutor's office was contacted and a request was made for the missing reports. In general, it was found that these reports were missing due to a change in prosecutors where the preceding prosecuting official neglected to inform his successor of this reporting responsibility. In other cases, the records were inaccessible. One prosecutor's report (Chautauqua County, New York) was received too late to be included in this wiretap report in which case the information will appear in the supplementary table of the 1976 report. If a report is not received from a judge, the Administrative Office contacts the authorizing judge for his report after receiving the prosecuting official's report.

Reports concerning wiretap authorizations were received from 80 state jurisdictions as well as the United States Department of Justice. The Administrative Office has the responsibility for matching the reports submitted by prosecuting officials with those filed by the authorizing judges and determining whether the information corresponds accurately. Increased cooperation between judges and prosecutors with regard to filing these reports has reduced reporting differences. The reporting numbers used in the appendix tables are reference numbers assigned by the Administrative Office of the United States Courts and do not necessarily correspond to the authorization or application numbers used by the reporting jurisdiction.

A. Nature of Intercepts:

For the 701 authorized orders, there were 676 prosecutor's reports, which included information on the average number of intercepts per day, the number of persons intercepted, the number of intercepts, and the number of incriminating intercepts. The other 25 authorized orders were never installed. The average number of intercepts varied in frequency from less than one per day to 428 per day. The average number of persons whose conversations were intercepted was 71 per order. The average number of conversations overheard was 654 per order. Almost one-half or 305 of the average number of communications intercepted produced incriminating evidence. A summary of the average number of intercepted conversations appears in Table 4.

Of the 676 installed orders, 620 were telephone wiretaps and 37 were microphone/eavesdrops. Nineteen reports from prosecutors specified both a telephone wiretap and a microphone/eavesdrop. (Table 6)

B. Cost of Intercepts:

The highest reported cost for a federal wiretap in terms of manpower, equipment, and other costs was $66,879 for a telephone wiretap in the Northern District of California. For state wiretaps the highest cost for a single authorization was $89,285 for an investigation conducted in Queens County, New York. The average cost for the 671 intercept orders for which a cost figure was reported was $6,970. This includes costs for orders where intercepts were never installed or never implemented but for which a cost was reported. A summary of the cost information appears in Table 5.

C. Arrests and Convictions:

Many of the criminal cases for which electronic surveillance was authorized in 1975 are still under active investigation. A total of 2,234 arrests had been made as of December 31, 1975 as a result of intercepts installed during calendar year 1975. There were 336 convictions in 1975, an increase of 88% from the 179 in 1974. Table 6 shows the type of intercept devices specified in the orders where installation was reported by prosecutors as well as the number of persons arrested and convicted as a result of these orders. Additional costs, arrests, trials, motions to suppress, and convictions resulting from 1975 intercepts will be reported by prosecutors in future supplementary reports.

V. Summary - June 1968 - December 1975

Table 7 summarizes for the period June 20 - December 31, 1968 and calendar years 1969 through 1975 information on authorized intercepts as to type of location and major offense. For authorizations where installation was reported by the prosecutor, Table 7 shows the average number of persons involved, the average number of incriminating intercepts, and cost information. Detailed data on applications for the interception of communications as reported in 1975 by the judges and prosecutors appears in the appendix tables which follow.

VI. Supplementary Reports

Title 18, U.S.C. §2519 requires supplementary reports to be filed by prosecuting officials concerning additional court or police activity occurring as a result of intercepts reported in prior years. All prosecuting attorneys who reported applications which appeared in previous years' reports were requested to provide supplementary reports showing any additional activity which took place during 1975 resulting from these orders.

During 1975 there were 1,915 arrests and 2,129 convictions reported as a result of authorized intercepts completed in prior years. The total number of arrests and convictions resulting from intercept orders installed in calendar years 1969 through 1975 is reflected in Table 14. Tables 8 through 13 summarize the additional police and court activity for intercepts installed in previous years.

The supplementary reports submitted by the United States Department of Justice included additional investigative and court activity not previously reported. A large amount of the activity reported in 1975 actually occurred in years prior to 1975; however, the information was not available in the previous years' reports. The additional data on arrests, trials, motions to suppress, and convictions appear in Table 14 under the year reported which is 1975. Appendix table A-2(federal) reflects the years during which the additional federal activity actually occurred.

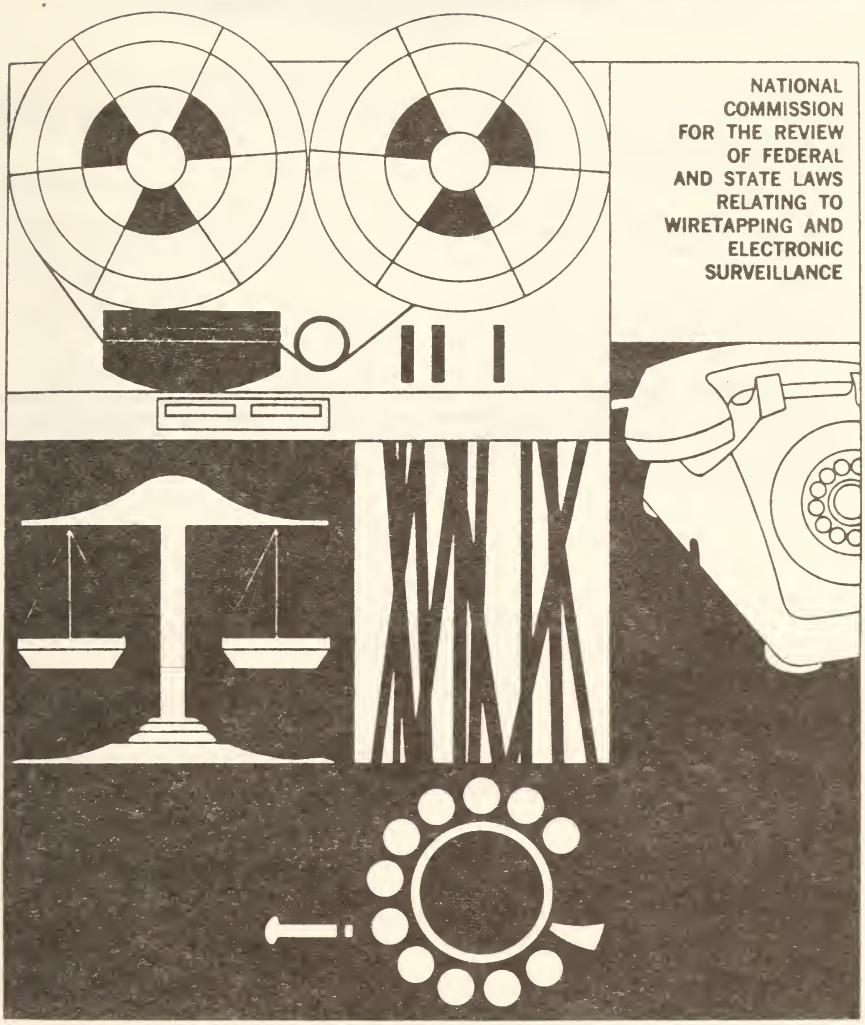
Many wiretap orders are related to large scale criminal investigations which cross county and state boundaries. Arrests, trials and convictions resulting from these interceptions often do not occur within the same year as implementation. Appendix tables A-2 (federal) and B-2 (state) describe in detail the additional activity reported by prosecuting officials.

Respectfully submitted,

Rowland F. Kirks
Director

April 30, 1976

Commission Studies



NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS
RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE
1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

April 30, 1976

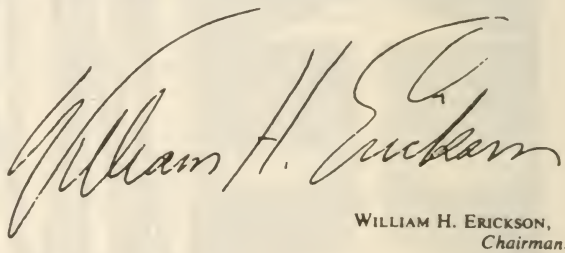
Honorable GERALD R. FORD,
President of the United States,
Washington, D.C.

Honorable NELSON A. ROCKEFELLER,
President of the Senate,
Washington, D.C.

Honorable CARL ALBERT,
Speaker of the House of Representatives,
Washington, D.C.

GENTLEMEN: In accordance with the provisions of section 804 of Public Law No. 351, Ninetieth Congress (Omnibus Crime Control and Safe Streets Act of 1968), as amended, the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance herewith submits its final report of findings and recommendations.

Respectfully yours,



WILLIAM H. ERICKSON,
Chairman.

Library of Congress Card No. 75-619447

STATE OF THE LAW OF ELECTRONIC SURVEILLANCE

Prepared by the Staff of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, September 1975.

CONTENTS

1. PRE-1968 ROOTS OF THE FEDERAL STATUTE
2. THE PRESENT LAW
   a. Provisions of the Federal Electronic Surveillance Statute
   b. State Statutes
   c. Constitutionality
   d. National Security Exception
   e. Consensual Surveillance Exception
   f. Other Interceptions Not Governed by Warrant Requirements
   g. Authorization of an Application for an Electronic Surveillance Order
   h. Judicial Approval of Electronic Surveillance Order
   i. Telephone Company Cooperation
   j. Designated Offenses
   k. Specification of Person to be Overheard
   l. Amendment of Orders
   m. Alternative Investigative Means
   n. Period of Interception
   o. Minimization of Interception
   p. Automatic Termination of Interception
   q. Additional Limitations on Issuance of Electronic Surveillance Orders
   r. Sealing and Custody of Records
   s. Notice of Interception
   t. Discovery
   u. Exclusionary Rule and Suppression of Evidence
      (1) Standing to bring the motion
      (2) Scope of the remedy
      (3) Appealability
   v. Use of Electronic Surveillance Evidence at Trial: Voice Identification and Transcripts
   w. Limitations on Use of Evidence Obtained by Electronic Surveillance in the States
   x. Limitation on Use of Evidence Obtained by Electronic Surveillance Outside the United States
   y. Illegal Eavesdropping—Criminal and Civil Cases
   z. Telephone Company Monitoring
3. MAJOR ISSUES ON THE LAW OF ELECTRONIC SURVEILLANCE

As used in this study "wiretapping" is the interception of communications transmitted over wire from a phone without the consent of a participant, while "bugging" is the interception of communications transmitted orally without the consent of a participant. "Electronic surveillance" is a generic term which includes both wiretapping and bugging, but is more frequently used as a substitute for the latter.

1. PRE-1968 ROOTS OF THE FEDERAL STATUTE

Eavesdropping's etymological structure discloses its origin. The practice of listening in with an unaided ear on the private conversations of neighbors was considered a common law nuisance. *See 4 W. Blackstone, Commentaries* 168 (Lewis ed. 1897). Meanwhile, the common law developed basic principles concerning the search of private property, eventually including the requirement that a judicial warrant be obtained authorizing a search. Taylor, *Search, Seizure and Surveillance*, pp. 24-6, published with another article as *Two Studies in Constitutional Interpretation* (1969). The warrant requirement itself was subject to refinement. The use of general warrants, which authorized a search without limits by British authorities in the American colonies, contributed to the adoption of the Fourth Amendment's requirement of particularity in arrest and search warrants. *See Osborn v. United States*, 385 U.S. 323 (1966) (Douglas, J., dissenting).

Wiretapping as a technological improvement on simple eavesdropping by the unaided ear came into being soon after the invention of the telegraph. Opposing forces in the Civil War tapped telegraph lines for military intelligence. Dash, Schwartz and Knowlton, *The Eavesdroppers*, 23 (1959). The states did not uniformly react to the practice: some prohibited wiretapping; others expanded existing laws against unauthorized disclosure of telegraphic messages; still others included the practice under malicious mischief statutes primarily designed to protect the property of wire communication companies. Many state legislatures simply ignored the problem. The invention of the telephone and the rapid growth of the telephone system, however, accentuated the problem. In 1916, a committee of the New York State Legislature found that the local police—in cooperation with the telephone company—had been tapping telephone lines in New York, although the practice was expressly prohibited by State law. New York Times, May 18, 1916, at 1, col. 1.

The first Federal laws proscribing wiretapping appeared as part of the national security program adopted during World War I. 40 Stat. 1017 (1918), 56 *Congressional Record* 10761-765 (1918). The statute was limited to the duration of the war and was intended solely for the protection of government secrets. After the war, agents of the Federal Bureau of Prohibition soon found the practice a useful law enforcement tool in apprehending bootleggers, and an appeal from a Volstead Act violation provided the factual setting for the first Supreme Court decision on the admissibility of wiretap evidence. *Olmstead v. United States*, 277 U.S. 438 (1928). The defendants had argued that wiretap evidence was constitutionally inadmissable because it violated the Fourth Amendment proscription of unreasonable searches and the Fifth Amendment ban against self-incrimination. The fact that this wiretapping was against the law of the state in which it took place was urged as an additional reason for a ruling of inadmissibility of such evidence. Chief Justice Taft, writing for the majority, rejected these contentions, noting that the Fourth Amendment protected only against seizures of tangible items and searches accomplished by physical invasions. The opinion stated that the Fourth Amendment was not violated by the wiretap because conversations were intangibles incapable of being seized, and that they had been obtained in this case by a process that did not involve a physical trespassory invasion of the defendant's premises. The Court found that there was no violation of the Fifth Amendment's self-incrimination provision in this instance because there had been no prior violation of the Fourth Amendment; the evidence, which had been obtained without infringement of Fourth Amendment protections, was not considered to be "compelled" testimony and thus did not fall within the Fifth Amendment's protection against self-incrimination. The objection to admissibility on the grounds of the State prohibition was dismissed with a conclusion that the Federal exclusionary rule was applicable only if a search and seizure violated the Constitution; otherwise the

common law rule permitting the admission of illegally secured evidence would be followed. The opinion did, however, note the possibility that the use of wiretapping evidence in criminal trials could be regulated by statute, should Congress choose to do so.

The opinions of Justices Brandeis and Holmes are the best remembered of four separate dissents. In 1890 Justice Brandeis had conceived of the idea of a right of privacy and had co-authored an article on the subject for the Harvard Law Review. 4 *Harv. L. Rev.* 193 (1890). That article is a recognized landmark in both constitutional and tort law. Now, in *Olmstead*, Justice Brandeis declared that his premised right of the individual to "be let alone" by the government demanded application of the Fourth Amendment protection against wiretapping. 277 U.S. at 478. The Fifth Amendment self-incrimination clause should operate to prevent the use of evidence uncovered by an illegal wiretap procedure. Justice Holmes, dismayed at a violation of the State law by Federal officers enforcing Federal law, termed wiretapping "dirty business," which lessened public respect for governmental integrity. 277 U.S. at 470.

Legislative proposals to limit the use of wiretap evidence in Federal trials were introduced in Congress in 1929 and again in 1931 but were never enacted. H.R. 5416, 71st Cong., 1st Sess. (1929); H.R. 9893, H.R. 5305, H.R. 23, 72nd Cong., 1st Sess. (1931). In 1934, however, Congress enacted the Federal Communications Act, generally regulating the communications industry and, in 1937, the Supreme Court ruled that a violation of Section 605 of that Act, which prohibited interception and divulgence of wire or radio communications, would bar the use at a Federal criminal trial of evidence obtained by Federal agents. *Nardone v. United States*, 302 U.S. 379 (1937). Two years later, in a case involving the same defendants, the Supreme Court ruled that evidence derived from information gained by wiretapping could not be used because of the prohibition of Section 605. *Nardone v. U.S.*, 308 U.S. 338 (1939)(referred to as Nardone II). The Supreme Court, on the same day as *Nardone II*, held that Section 605 was applicable to both intrastate as well as interstate communications. *Weiss v. United States*, 308 U.S. 321 (1939). But a later opinion held that testimony which was elicited from a witness by showing him transcripts of his incriminating telephone conversations could be admitted into evidence against persons not parties to the conversation. These persons were ruled not to have standing to object to the evidence. *Goldstein v. United States*, 316 U.S. 114 (1942).

The Department of Justice construed *Nardone* I and II as not prohibiting the interception of wire communications *per se*, but only the interception *and* divulgence of their contents. The Supreme Court never explicitly ruled on this position, and the Department continued to authorize wiretapping until March 1940, when then-Attorney General Robert H. Jackson prohibited it. Less than three months later the threat to the national security from the activities of foreign agents during World War II (the "fifth column") brought a letter by President Roosevelt to Jackson authorizing and directing that wiretapping and bugging be used in checking such activities.

In 1942, the Supreme Court ruled that searches by electronic bug were not within the scope of the Fourth Amendment protections, absent any trespass onto the premises searched. *Goldman v. United States*, 316 U.S. 129 (1942). Government agents had obtained evidence by placing a device known as a detecta-phone against the common wall of an adjoining office. Further, Section 605 of the Federal Communications Act was found not to control this practice because there were no "communications" or "interceptions" as defined by the statute. *Goldman* was the first of a line of cases in which the Court distinguished wiretapping from other forms of electronic eavesdropping because Section 605 regulated only wiretapping.

The distinction between wiretaps and bugs, based on statutory interpretation, was to remain the law for the next 25 years. The question that received major consideration in several Supreme Court decisions during this interval was the effect of the Federal statute on the States. Initially, the Court determined that Section 605 governed only the use of evidence in Federal courts, so that evidence obtained in violation of the statute could be received by State courts. *Schwartz v. Texas*, 344 U.S. 199 (1952). The Court reaffirmed this holding almost 10 years later. *Pugach v. Dollinger*, 365 U.S. 458 (1961). However, Federal courts were not permitted to accept evidence obtained in wiretaps conducted by State law enforcement officers which violated Section 605. *Benanti v. United States*, 355 U.S. 96 (1957). The *Schwartz* decision was finally overruled in *Lee v. Florida*, 392 U.S. 378 (1968), decided after the Supreme Court had already repudiated *Olmstead* and placed electronic surveillance within the scope of the Fourth Amendment. In *Lee* the Court decided that the rationale given to justify admission into State criminal trials of evidence obtained in violation of Section 605 was no longer supported by viable case law. The Court noted that the *Benanti* decision represented a recognition of the broad scope of Section 605's protection against

the divulgence of intercepted conversations. Further, by this time *Wolf v. Colorado*, 338 U.S. 25 (1949), which had left to the states the determination of whether evidence seized in violation of Federal law would be admissible in State courts, had been explicitly overruled by *Mapp v. Ohio*, 367 U.S. 643 (1961). In *Mapp* the Court had held that evidence obtained by State officers in an unreasonable search is inadmissible in a State criminal trial because Fourth Amendment protections extended to citizens through the agency of the 14th Amendment's due process clause.

Further, the trespassory invasion theory of *Olmstead*, affirmed in *Goldman*, was limited by subsequent decisions of the Court. In *Irvine v. California*, 347 U.S. 128 (1954), the Court refused to overturn a conviction secured by State officers with evidence derived from recording defendant's conversations with the aid of microphones concealed in the wall of the defendant's home, but this result was based on a declaration that *Wolf v. Colorado* left the determination of admissibility of evidence to the states. In its decision, the Court condemned the investigative practice followed, using language to indicate that conversations were tangible items protected by the Fourth Amendment. In *Silverman v. United States*, 365 U.S. 505 (1961), the Court held that evidence was inadmissible which was obtained from a spike mike driven through the party wall of an adjoining dwelling to make contact with a heating duct in defendant's house that conveniently served as a transmitter of all conversations. The Court based this holding on the invasion of defendant's property by the spike. Justice Douglas' concurring opinion in *Silverman*, which spoke not of the trespass involved but of the invasion of the privacy of the home, was an indication of the evolving idea of the individual's right to privacy. And two years later the court refused to hold admissible evidence in a case where the device intruded into the adjoining wall only as much as a thumbtack. This decision was given without an opinion, the Court making no attempt to reconcile this case with *Goldman*. *Clinton v. Virginia*, 377 U.S. 158 (1963).

Meanwhile, a line of decisons recognized consensual exceptions to Section 605 of the Federal Communications Act that would later be legislatively incorporated into Title III. These decisions also indicated a move away from the trespass doctrine, and toward a theory of privacy. In *On Lee v. United States*, 343 U.S. 747 (1952), the Court rejected the argument that conversations that were transmitted by a device hidden on a government informant were inadmissible because consent to his entry into the portion of defendant's laundry that was open to the public had been obtained by fraud and thus constituted a trespass. Such recordings were admissible as they violated neither the Fourth Amendment nor Section 605 of the Federal Communications Act. In *Rathbun v. United States*, 355 U.S. 107 (1957), the Court ruled that police who obtained evidence by overhearing telephone conversations through the use of a regularly used extension telephone with the consent of one of the parties to the conversation did not violate Section 605. The "wired agent" situation was the factual basis of *Lopez v. United States*, 373 U.S. 427 (1963), wherein the Court held that use of a hidden recorder by a government agent did not violate the Fourth Amendment because the defendant had in fact risked disclosure of his bribe attempt by making it to another person. But Justice Brennan's dissent stressed a belief that all electronic surveillance should be pre-conditioned upon antecedent justification before a magistrate, a concept central to the Fourth Amendment's requirement of reasonable searches. In 1966 the Court once again approved the use of a hidden recorder on a government agent to secure evidence of jury tampering. *Osborn v. United States*, 385 U.S. 323 (1966). The Court, however, emphasized that the surveillance was executed with previous judicial authorization and ongoing judicial supervision, thus meeting Justice Brennan's key objection in *Lopez*. The surveillance procedures used in *Osborn* were later lauded in *Berger v. New York*, 388 U.S. 41 (1967), for meeting the Fourth Amendment's demand for particularity as a prerequisite to recognition of a reasonable search and seizure. Another case decided the same year as *Osborn* showed the blurring outlines of the Court's definition of the individual's right to privacy. Although it spoke of constitutionally protected areas, the Court was more concerned with the degree of security relied upon by the defendant when speaking within such an area and held that "relying upon his misplaced confidence that (the informant) would not reveal his wrongdoing" was not justified. *Hoffa v. United States*, 385 U.S. 293 (1966).

The trespass doctrine was finally abandoned, and an expectation of privacy test explicitly adopted, in the two cases decided in 1967: *Katz v. United States*, 389 U.S. 347, interpreted the protection offered by the Fourth Amendment to include protection against an invasion of privacy, which was deemed to be unreasonable without a search warrant; and *Berger v. New York*, 388 U.S. 41, outlined the criteria such a warrant should meet to be within Fourth Amendment standards of particularity.

The judicial life of *Olmstead's* concept of a trespassory invasion that centered Fourth Amendment protection on places rather than persons was

definitely ended in *Katz*. FBI agents had attached a bugging device to the exterior of a telephone booth used by the defendant in his gambling operations. This device was activated only when the defendant was in the booth. The defendant contended that the government had violated a constitutionally protected area. The Court granted a reversal, but did not use its trespassory invasion theory on which the defendant had relied; instead, the Court declared that the Fourth Amendment protects persons who justifiably rely on a reasonable expectation of privacy.

Berger spelled the end for then-existing non-consensual electronic surveillance practices in State law enforcement. The Court found constitutional deficiencies in a New York statute authorizing both court-ordered wiretapping and bugging. The absent Fourth Amendment safeguards included a failure to particularly describe or list: 1) the place to be searched and the person whose conversation was to be seized; 2) the crime that had been or was being committed; 3) the nature of the conversation being seized; 4) what limitations the officers executing the order must observe so as not to search unauthorized areas or continue after the object of the search had been seized, thus in effect allowing a general search; 5) the dispatch by which the order should be executed; 6) a requirement that the officer executing the order make a return to the court issuing the order to show what had been seized; 7) those exigent circumstances that mandated the absence of prior notice to persons whose privacy had been invaded. These deficiencies, the Court held, combined to empower *carte blanche* eavesdropping without adequate judicial supervision. The New York law thus promoted a general search inherently violative of the Fourth Amendment's ban on unreasonable searches and seizures. The inference drawn from this decision, however, was that electronic eavesdropping would be within accepted Fourth Amendment bounds when requirements of particularity were included within a scheme of statutory provisions which allowed an adequate degree of judicial approval and supervision.

The holdings of *Katz* and *Berger* are the basis for much of the contents of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. *Berger* and *Katz* appeared when the evil impact of organized crime on American society was made apparent by several Congressional and Executive Commission investigations. The extent of the impact of such activity on American society was vigorously publicized with the issuance of *The Challenge of Crime in a Free Society: The Report of the President's Commission on Law Enforcement and the Administration of Justice* (1967). That report concluded that wiretapping and bugging were necessary to combat organized crime operations, because the secrecy and impenetrability of organized crime prevented the success of other means of investigation. New York prosecutors, using the state's electronic surveillance law, claimed that that method of investigation could be effective against organized crime. Legislative proposals for Federal wiretapping powers had been made in earlier years, but the precipitating events—recognition of the magnitude of the organized crime problem and definition of Constitutional limits—focused in 1968, the year a comprehensive law on electronic eavesdropping was finally enacted.

2. THE PRESENT LAW

a. Provisions of the Federal Electronic Surveillance Statute

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (hereinafter, the legislation generally will be referred to as "Title III"; sectional references are to the sections of Title III as enumerated in Title 18 of the United States Code) serves dual purposes: (1) the protection of privacy of wire and oral communications; and (2) a uniform delineation of the circumstances and conditions for the authorized interception of oral and wire communications. Senate Report No. 1097, reprinted at 1968 *U.S. Code Cong. & Ad. News* 2153. The statute generally prohibits wiretapping and bugging unless a party to the conversation intercepted gives his consent. 18 U.S.C. 2511(1). The manufacture, distribution, possession and advertising of wire or oral communication intercepting devices is also prohibited. 18 U.S.C. 2512. These devices may be seized and confiscated by the United States. 18 U.S.C. 2513. Exceptions are made for communications services needs, and for Federal or State government officials in the normal course of their activities. 18 U.S.C. 2512(2).

A maximum fine of $10,000 or a maximum prison term of five years, or both, may be imposed for violation of these provisions. 18 U.S.C. 2512(1). Victims of illegal eavesdropping are given the right to bring a civil cause of action and recover either actual damages or a fixed rate of liquidated damages, in addition to punitive damages and attorney's fees and costs against any person who illegally intercepts, discloses, or uses, wire or oral communications or procures any other person to perform such actions. 18 U.S.C. 2520.

The procedures contained in Title III for obtaining court authorization for interception of wire and oral communications were enacted to aid law en-

forcement agencies in combatting organized criminal activity. Sections 2516(1) and 2518 set forth procedures that Federal agencies must follow to obtain court orders to use electronic surveillance in investigating a specified list of offenses. Sections 2516(2) and 2518 establish minimum standards to be observed by States choosing to enact legislation permitting court ordered electronic surveillance, although the States may adopt more restrictive standards than those found in Title III. They further specify that court-ordered electronic surveillance may be used for law enforcement purposes only in those States enacting such authorizing legislation.

Law enforcement agencies must observe the procedural standards of Title III in obtaining and executing surveillance orders. A failure to meet these guidelines enables any aggrieved person to invoke a statutory right of suppression. 18 U.S.C. 2515, 2518(10).

Section 2518(7) states an exception to the requirement that a warrant must be obtained before a non-consensual interception can be carried out. This provision permits warrantless interceptions in certain emergency situations in which there is probable cause to issue a warrant but a warrant cannot "with due diligence" be obtained, provided that application for a warrant is made within 48 hours of the beginning of the interception. This provision has never been used by Federal officers, however, although equivalent provisions in state statutes (e.g. New Jersey and Delaware) have been used on several occasions.

The statute requires that an annual report be submitted by the Director of the Administrative Office of the United States Courts to the Congress, containing statistical information submitted from all judges and law enforcement officials who authorize or apply for electronic surveillance orders. 18 U.S.C. 2519. A long-range and more detailed evaluation of the effect of the statute in aiding law enforcement and in protecting privacy is to be provided by the six year comprehensive study by the Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, which was established by Section 804 of Title III.

b. State Statutes

By the end of 1974, a total of 22 States and the District of Columbia had provided statutory procedures for court-approved electronic surveillance for criminal investigations that were consistent with Title III standards (Arizona, Colorado, Connecticut, Delaware, Florida, Georgia, Kansas, Maryland, Massachusetts, Minnesota, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, Oregon, Rhode Island, South Dakota, Virginia, Washington, Wisconsin). While some jurisdictions adopted the Title III procedures almost verbatim, there have frequently been variances in State legislation, reflecting local efforts to account for differences in the structure of the State judiciary as well as the needs of local law enforcement. Some States have adopted standards considerably more restrictive than those of Title III. The statute adopted in the State of Washington, and a statute adopted in Pennsylvania in 1975, are so restrictive, in fact, as to make electronic surveillance a relatively impractical tool in law enforcement.

c. Constitutionality

The Supreme Court has issued six opinions in cases interpreting Title III standards on electronic surveillance since the 1968 passage of the Act. *United States v. Chavez*, 416 U.S. 562 (1974); *United States v. Giordano*, 416 U.S. 505 (1974); *United States v. Kahn*, 415 U.S. 143 (1974); *Gelbard v. United States*, 408 U.S. 41 (1972); *United States v. United States District Court*, 407 U.S. 297 (1972); *Alderman v. United States*, 394 U.S. 165 (1969). The Court has declined the opportunity to consider any cases challenging the constitutionality of the statute. *Dicta* affirming the constitutionality of Title III have appeared in majority opinions interpreting non-constitutional aspects of the statute and have been deemed strong indicators of a Court view of the Act's constitutionality. For example, Justice Powell's statement in *United States v. United States District Court* is often used to advance this claim:

> The Act [Title III] represents a more comprehensive attempt by Congress to promote a more effective control of crime while protecting privacy of individual thought and expression. Much of Title III was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court in *Berger* and *Katz*. 407 U.S. 297, 302 (1972).

Justice Douglas is the only member of the Court who has made a statement indicating a belief that the Act is unconstitutional, an announcement consistent with previously expressed views that electronic surveillance necessarily constitutes a general search inherently violative of the Fourth Amendment. *Cox v. United States*, 406 U.S. 934 (1972) (Douglas, J., dissenting from a denial of certiorari).

Nine of the eleven circuits of the Federal Courts of Appeals have affirmed the constitutionality of the Act. All but one of the Federal District Court opinions considering a constitutional challenge have upheld the statute. The sole exception, *United States v. Whitaker*, 343 F. Supp. 358 (E.D.Pa. 1972), was promptly reversed by the Third Circuit.

474 F.2d 1246 (3rd Cir. 1973), *cert. denied*, 412 U.S. 953 (1973).

Constitutional challenges to Title III have rested on legal theories grounded in the First, Fifth, Sixth, Ninth, and Fourteenth Amendments, and the concept of a "penumbral right" of privacy enunciated in *Griswold v. Connecticut*, 381 U.S. 479 (1965). Generally, however, the attack is by the avenue of the Fourth Amendment's prohibition against unreasonable searches and seizures, and judicial opinions have discussed constitutionality only within this traditional framework.

Fourth Amendment challenges have advanced varying arguments on the constitutional propriety of court-approved electronic surveillance. The absolutist position contends that electronic surveillance is a general search inherently outside the pale of constitutionality. A second position recognizes that electronic surveillance can be constitutionally valid when certain procedural safeguards such as those discussed in *Berger* are present; however, it is then argued that Title III's provisions fail to meet these constitutional requirements.

Federal courts have dismissed the absolutist argument by noting that the Supreme Court in *Berger* and *Katz* expressly held some forms of electronic surveillance to be constitutional if accompanied by appropriate procedural safeguards. *See, e.g., U.S. v. Cox*, 462 F.2d 1293 (8th Cir. 1972), *cert. denied*, 417 U.S. 918 (1974). The argument that the statute fails to provide these safeguards is met by the fact that the Supreme Court laid down, in *Berger* and *Katz*, the essential requirements in any statute or rule authorizing electronic eavesdropping. Congress, it has been held, included these standards in drafting Title III. *United States v. Cox*. 449 F.2d 679 (10th Cir. 1971), *cert. denied*, 406 U.S. 934 (1972). For example, in the Eighth Circuit *Cox* opinion, the court matched the requirements of particularity and judicial supervision mandated in *Berger* and *Katz* with specific provisions found in Title III. 462 F.2d at 1303. Ample precedent on the constitutionality of Title III has developed, so that the most recent decisions tend to rely on the prior authority without further analysis.

Often, a finding of constitutionality of a State law is based on the fact that the State law is modeled on Title III, which conforms to the constitutional requirements set forth by the Supreme Court in the *Berger* and *Katz* decisions. However, the Maryland Court of Appeals, faced with a challenge of a State statute that was passed before the enactment of Title III, stressed that the Maryland law was sufficient authorization to allow electronic surveillance by State officials, but in instances where the State law is not as explicit as Title III, the stricter standards of the latter must be followed in determining the legality of interception by State officials. *State v. Siegel*, 266 Md. 256, 292 A.2d 86 (1972).

d. National Security Exception

The closest the Supreme Court has come to dealing with the constitutionality of Title III is in the area of national security. The validity of warrantless electronic surveillance against domestic subversive groups under a national security rationale was examined by the Supreme Court in the case of *United States v. United States District Court*, 407 U.S. 297 (1972) (often called the *Keith* case, after the Federal judge in the Eastern District of Michigan who had held the practice to be invalid). The Court held that wiretapping of a "domestic organization," defined as a "group or organization . . . composed of citizens of the United States and which has no significant connections with a foreign power, its agents or agencies," without a prior judicial warrant was unconstitutional. 407 U.S. at 309 n.8. In reaching its decision the Court left open the question of whether the warrant requirement of the Fourth Amendment governed the President's power to order surveillance of the agents and agencies of foreign powers, both in this nation and abroad. It also noted that Section 2511(3) of Title III, which states that the statute shall not limit the powers of the President with respect to national security, served merely as a disclaimer of any congressional intent to legislate with respect to national security surveillance. 407 U.S. at 307-308.

More recently, the Supreme Court abstained from answering the question whether Presidential power to order surveillance of foreign agents and agencies whose activities affected the national security came outside the dictates of the Fourth Amendment's warrant clause by declining review in *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974), *cert. denied*, 419 U.S. 881 (1974). The Third Circuit, in an *en banc* decision, had held that search by electronic surveillance, when based on the exigent needs of national security, was not unreasonable under the Fourth Amendment and could thus be excepted from the warrant requirement. Earlier cases such as *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971), based the President's power to order such surveillance on the special Executive prerogatives in the foreign affairs area that had been announced in *United States v. Curtiss Wright Export Corp.*, 299 U.S. 304 (1936). However, the United States Court of Appeals of the District of Columbia Circuit, in a most recent major ruling, has held that a warrant must be obtained to wiretap a domestic organization, even in circum-

stances involving national security, when the organization is not an agent of or in collaboration with a foreign power. *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975). Although the holding of the case was limited to requirements for surveillance of a domestic organization, the court went on to state the belief that in the absence of exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional. Legislative hearings have been held in recent years on the subject of warrantless national security surveillance and bills are before committees in the Congress that would establish a warrant procedure in this area.

e. Consensual Surveillance Exception

The Supreme Court in *United States v. White*, 401 U.S. 745 (1971), ruled, by plurality opinion, that the use of a hidden body recorder by one party to a conversation did not violate the Fourth Amendment. This ruling has been followed in subsequent cases, with the exception of a recent opinion of the Michigan Supreme Court adopting the dissent of Justice Harlan in *White*. *People v. Beavers*, 393 Mich. 554, 227 N.W.2d 511 (1975), *petition for cert. filed*, 17 Crim.L.Rep. 4131 (U.S. July 5, 1975) (No. 75-21). Title III generally allows such recordings by both law enforcement officers and private individuals when used for non-tortious purposes. This is the prevailing rule in most states.

Eleven states, however, have enacted statutes either limiting or prohibiting one-party consent recording except for telecommunications service monitoring. These statutes are, in their efforts to make exceptions to the general proscriptions, varied and somewhat confusing. Some of the apparent distinctions, indicated by the language of the statutes, are outlined in this paragraph. The most restrictive of these statutes, that of Pennsylvania, permits no recording of conversations without the consent of all parties; even law enforcement authorities must obtain a court order for a one-party consensual interception, and can do so only in situations endangering the safety of law enforcement officers. Even with a court order, the authorities may not record the conversations. The State of Washington, too, requires law enforcement authorities to obtain a court order for one-party consent recordings and permits them only for investigation of crimes dangerous to life; even then the recordings would not be admissible in evidence except in national security cases. New Hampshire permits recording only with the consent of all parties, except for law enforcement purposes under a court order. Two states, California and Ohio, make exceptions to their requirement of consent of all parties, allowing one-party consent monitoring without a court order in the interest of preventing or detecting crime. Georgia requires a court order for one-party consent interception by law enforcement, unless a crime is actually being committed, when no court order is necessary. Two other states, Massachusetts and Michigan, permit law enforcement officers in the performance of their duties to record one-party consent conversations without a court order. Montana permits recording by public officials in the course of their duties. Further, persons given warning or speaking at public meetings may be recorded. Both Oregon and Maryland make a distinction between telecommunications, for which the consent of one party is sufficient, and other surrepititious electronic surveillance, which demands the consent of all parties. Law enforcement authorities in these states need a court order, except that in Oregon no court order is necessary for a law enforcement officer to record, with one-party consent, in a narcotics investigation. Further, in Oregon, conversations in a public office or penal institution may be recorded by the public officials in charge.

In a somewhat unusual decision, the Wisconsin Supreme Court has interpreted the Wisconsin statute, which was patterned after Title III, to mean that the results of any electronic interceptions will not be admitted as evidence without the consent of the party against whom it is to be used unless a court order was obtained for the interception. In reaching this result, the court made a distinction between one-party consent interception, which is permitted by the Wisconsin statute, and use as evidence of information gained through such interception. *State ex rel. Arnold v. County Court*, 51 Wis.2d 434, 187 N.W.2d 354 (1971).

In those states recognizing the Title III type statutory exception for consensual interception, that exception has been held to extend to police officers playing investigative roles. Thus, police entry into a suspect's unoccupied apartment and subsequent recording of conversations after answering the phone and assuming the identity of the suspect was proper without an order authorizing interception of the conversations. *State v. Vizzini*, 115 N.J. Super. 97, 278 A.2d 235 (1971); *see also Commonwealth v. Todisco*, 294 N.E.2d 860 (Mass. 1973) (allowing police, after entry with a warrant, to test telephone for possible illegal use.).

f. Other Interceptions Not Governed by Warrant Requirements

Title III by its terms protects oral communications uttered under an expectation that they are not subject to interception under circumstances justify-

ing such expectation. 18 U.S.C. 2510(2). It also, more generally, protects wire communications. Following these definitional boundaries, the Ninth Circuit has held that an automobile radio-telephone communication can be intercepted when it is transmitted over the air, thus negating defendant's expectation of privacy, but when it is transmitted to a land line telephone it will be given statutory protection on the grounds that all communications carried in whole or part by a common carrier will be treated as wire communications. *United States v. Hall*, 488 F.2d193 (9th Cir. 1973). This seemed, however, a strained interpretation of Title III. As the dissenting judge in this case noted, the communication in question fell within the prohibitions of Section 605 of the Federal Communications Act, and the same conclusion could have been reached without application of Title III to this situation.

In a case where police officers overheard one end of a telephone conversation without using any mechanical devices, the Seventh Circuit ruled that an "interception" had not occurred. *United States v. McLeod*, 493 F.2d 1186 (7th Cir. 1974). However, using a device to record such a conversation without any party's consent brings it within the definitions of Title III, but since it is an "oral" rather than a "wire" interception it is only prohibited if in violation of the speakers' reasonable expectation of privacy. *United States v. Carroll*, 337 F.Supp. 1260 (D.D.C. 1971). The court in *Carroll* outlined some tests for evaluating whether interception of an oral communication constitutes an offense under Title III: 1) whether the speakers reasonably believe their conversations cannot be overheard, and 2) whether the listener, considering the circumstances, would find the speakers' belief justified; these two subjective standards must be considered in light of a more reliable objective standard, 3) whether *in fact* the listener was able to hear the conversation unaided by a mechanical device, and if so, whether the hearing was contrived by the listener—whether he placed his ear, by trespass or otherwise, in an unusual or improper position. Concerning another aspect of expectation of privacy, the Second Circuit has held that defendants who were in their former apartment where an eavesdropping device had been installed with the permission of the present tenants had no expectation of privacy within a stranger's apartment. *United States v. Pui Kan Lam*, 483 F.2d 1202 (2d Cir. 1973), *cert. denied*, 415 U.S. 984 (1974).

Other distinctions as to what type of interception is governed by warrant requirement have proved equally troublesome and have resulted in inconsistent rulings in Federal courts. In *United States v. Luna*, Crim. No. 49331 (E.D. Mich., Jan. 25, 1974), non-telephonic background conversations inadvertently overheard in the course of a warranted wiretap were upheld as properly admissible in evidence, pursuant to the "plain view" doctrine of search and seizure law, which holds that evidence inadvertently discovered during the course of a proper search may be seized. However, an earlier opinion decided that background conversations not described by the surveillance order fell outside the limits of particularity demanded by the Constitution and must be suppressed as improper, within the terms of the Fourth Amendment requirement. *United States v. King*, 335 F.Supp. 523 (S.D.Cal. 1971), *modified*, 478 F.2d 494 (9th Cir. 1973), *cert. denied*, 417 U.S. 920 (1974). The court in *Luna* distinguished the *King* decision by noting that the agents in *King* actively sought to "seize" the background conversations and thus could not invoke the plain view doctrine.

Title III and most similar state laws contain an exception for operators and other communications carrier employees to engage in what has been commonly termed "service monitoring." 18 U.S.C. 2511(2)(a)(i). If a crime is overheard by a service monitoring operator during the ordinary course of business, then evidence from such an overhearing is admissible in evidence. *State ex rel. Flournoy v. Wren*, 108 Ariz. 356, 498 P.2d 444 (1972); *People v. Sierra*, 343 N.Y.S.2d 196 (Sup. Ct. 1973); *see also Williams v. State*, 507 P.2d 1339 (Okla. Crim. 1973).

Another exception arises from the definition of intercepting device; the prohibited devices do not include a telephone "being used by the subscriber or user in the ordinary course of its business." 18 U.S.C. 2510(5)(a)(i). Most courts have held that the purposeful use of an extension telephone or a party line to surreptitiously record a private conversation does not come within the ordinary-course-of-business exception and must be suppressed as an illegal interception. *United States v. Harpel*, 493 F.2d 346 (10th Cir. 1974); *United States v. Banks*, 374 F.Supp 321 (D.S.D. 1974); *People v. Tebo*, 37 Mich. App. 141, 194 N.W.2d 517 (1971). *Contra*, *United States v. Christman*, 375 F.Supp. 1354 (N.D.Cal. 1974).

Title III governs only the *aural acquisition* of the contents of any wire or oral communication by any electronic, mechanical, or other device. In several cases defendants have argued that the use of pen registers and touch-tone decoders—devices which record all phone numbers dialed from a particular phone, but do not intercept the conversation—should be under a warrant procedure. A Florida telephone company has appealed a District Court order authorizing installation of a pen re-

gister under Rule 41 (regular search warrant procedure) of the Federal Rules of Criminal Procedure, arguing, among other things, that use of pen registers should be included under Title III warrant procedures *Southern Bell v. United States*, Civil Nos. 74-3357 and 74-3358 (5th Cir., filed Sept. 16, 1974). Courts have not, up to this time, adopted this position, however, but have relied on the statement in the legislative history of Title III that ". . . the use of a 'pen register' (without a warrant) for example would be permissible." *In re Korman*, 351 F.Supp. 325 (N.D. Ill. 1972), *aff'd*, 486 F.2d 926 (7th Cir. 1973). However, a Massachusetts opinion has held that the use of a pen register, although not governed by Title III, is prohibited by Section 605 of the Federal Communications Act. *Commonwealth v. Coviello*, 291 N.E.2d 416 (Mass. 1973). A recent Eighth Circuit opinion disagrees with *Coviello*, concluding that pen register use is governed neither by Title III nor by the Federal Communications Act. *United States v. Brick*, 502 F.2d 219 (8th Cir. 1974). In any event, the American Telephone and Telegraph Company (AT&T) maintains a policy against supplying information necessary to install a pen register absent a court order. Further, even with a court order, telephone companies have pressed for full application of Title III standards. In a recent case, the refusal of an AT&T security officer to give information on the basis of an order for a pen register which did not comply with Title III standards was held not to constitute contempt of court. The security officer had offered to cooperate but believed he had no authority under telephone company policy. If there was any contempt, a matter which the court did not resolve, it was by the telephone company, not its employee, but no charge of contempt had been brought against the company. *In re Joyce*, 506 F.2d 373 (5th Cir. 1975).

There has been no difficulty with the concept that if a valid wiretap order has been issued, the use of a pen register is comprehended within the terms of that order, so that a separate authorization is not needed. *United States v. Falcone*, 505 F.2d 478 (3d Cir. 1974), *cert. denied*, 420 U.S. 955 (1975).

While Title III will cover the audio portion of a videotape, the visual portion is not subject to suppression for nonstatutory compliance, because the statute does not cover photographic surveillance. *Sponick v. City of Detroit Police Department*, 49 Mich. App. 162, 211 N.W.2d 674 (Mich. Ct. App. 1973). Similarly, use of an electronic transmitting device, commonly called a "bumper beeper," that is placed on a suspect's car to monitor the car's movements is outside the scope of Title III. But courts have held that use of "bumper beepers" is not outside protection of the Fourth Amendment. *United States v. Holmes*, Gainesville Crim. No. 73-27 (N.D. Fla. April 24, 1974), *United States v. Martyniuk*, —F.Supp.—, 17 Crim. L. Rep. 2215 (D.Ore. May 20, 1975). The results in these cases (the Holmes case is currently on appeal) are open to question in light of the Supreme Court's plurality ruling in *Cardwell v. Lewis*, 417 U.S. 583 (1974), that the taking of paint scrapings from the exterior of the defendant's automobile upon probable cause was reasonable and invaded no right of privacy that the requirement of a search warrant is meant to protect.

g. Authorization of an Application for an Electronic Surveillance Order

Title III specifies that the Attorney General of the United States, or any Assistant Attorney General specially designated by him, may authorize an application for an order permitting the interception of wire or oral communications. 18 U.S.C. 2516(1). The commentary in the legislative history on this section explains that "(t)his provision centralizes in a publicly responsible official subject to the political process the formulation of law enforcement policy on the use of electronic surveillance techniques. Centralization will avoid the possibility that divergent practices might develop. Should abuses occur, the lines of responsibility lead to an identifiable person. This provision in itself should go a long way toward guaranteeing that no abuses will happen." 1968 *U.S. Code Cong. & Ad. News* 2153, at 2185. The commentary on Section 2516(2), relating to State laws, notes that State legislation enacted in conformity with this chapter should specifically designate the principal prosecuting attorneys empowered to authorize interceptions. Id. at 2187.

In 1974 the Supreme Court issued two decisions that examined incidents of noncompliance with the authorization provisions found in Section 2516(1) of Title III. In *United States v. Giordano*, 416 U.S. 505 (1974), the Court found that applications authorized by the Attorney General's Executive Assistant, signing the Attorney General's initials, violated the procedure mandated by Section 2516(1) and that evidence obtained under such an order or an extension thereto was inadmissible and could be suppressed under 18 U.S.C. 2515. The Supreme Court's ruling in *Giordano* sought to "directly and substantially implement the Congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device." 416 U.S. at 527. In a companion case,

United States v. Chavez, 416 U.S. 562 (1974), however, the Court found that a *misidentification* on an application that listed an Assistant Attorney General as the officer authorizing taps that were actually approved by the Attorney General did not require suppression.

Lower court opinions prior to these two decisions had reached divergent results in considering similar factual situations. Federal and State courts since have been faced with the task of reconsidering a multitude of cases in which wiretap evidence stemmed from orders based on improperly authorized applications. It would be difficult to prosecute any of those cases in which evidence was suppressed pursuant to *Giordano*, as the Government would have the burden of showing that evidence for subsequent prosecution was not derived from information gained during the unauthorized tap. In effect, the government may be forced to begin its investigations anew in many cases to comply with Constitutional requirements and build an independent and untainted case against the offender.

Courts now must also deal with issues of proof of the authenticity of official signatures on intercept orders. *United States v. Thomas*, 508 F.2d 1200 (8th Cir. 1975). *Giordano* and *Chavez* have also opened up related issues concerning whether noncompliance with other aspects of the statute are serious enough to require suppression of the evidence. *See United States v. Donovan*, 513 F.2d 337 (6th Cir. 1975) (Inventory notice); *United States v. Bernstein*, 509 F.2d 996 (4th Cir. 1975) (Identification of persons under surveillance in order).

The major authorization problem in State courts has been to determine the propriety of authorization by assistants acting in lieu of the chief prosecutor of a state or a geographical subdivision. One State court has held that an Assistant State's Attorney could authorize a wiretap under a statute giving such authority to a State's Attorney, because the State Constitution, as it existed at the time the State wiretap act was adopted, granted Assistant State's Attorneys full authority to do and perform any official act that the State's Attorney could do. *State v. Angel*, 261 So.2d 198 (Fla. Ct. App. 1972), *aff'd*, 270 So.2d 715 (1972). In Kansas, the State electronic surveillance statute gave express application authority to Assistant Attorneys General, but did not mention Assistant County Attorneys. The Kansas Supreme Court held a wiretap order invalid applying the doctrine of *expressio unius est exclusio alterius* (absence of items in a legislative list shows an intent to exclude). The Court read the State statute to strictly limit the class of persons who could apply for electronic surveillance orders. *Application of Olander*, 213 Kan. 282, 515 P.2d 1211 (1973). The Minnesota Supreme Court in a similar ruling, based on an *expressio unius* interpretation of the statute and on the authority of the Fourth Circuit's decision in *Giordano* (the decision later affirmed by the Supreme Court), held that the State and Federal statutes prohibited an Assistant County Attorney from authorizing an application. *State v. Frink*, 296 Minn. 57, 206 N.W.2d 664 (1973). The *Giordano* decision also mandated a conclusion that an Assistant District Attorney could not make a valid statutory application in *Price v. Goldman*, 525 P.2d 598 (Nev. 1974). A New Jersey ruling established that an acting prosecutor, if properly appointed to exercise all of the duties of the office of prosecutor, can authorize wiretap applications in the absence of the chief prosecutor. *State v. Travis*, 125 N.J.Super. 1, 308 A.2d 78 (Essex County Crim. Ct. 1973); *aff'd*, 133 N.J. Super. 326, 336 A.2d 489 (N.J. App. Div. 1975). However, such power could not be delegated if the chief prosecutor was not actually absent from the jurisdiction. *State v. Cocuzza*, 123 N.J. Super. 14, 301 A.2d 204 (Essex County Crim. Ct. 1973). A New York court, faced with a suppression motion where an application had been made by an Assistant District Attorney, denied the motion, holding that State law allowed a District Attorney to designate a particular assistant to exercise the powers and duties of the office in the event of a vacancy or when the District Attorney is absent or disabled. *People v. Fusco*, 75 Misc.2d 981, 348 N.Y.S.2d 858 (Nassau County Ct. 1973).

The key to the authorization issue seems to be that a high-ranking, publicly-responsible official take responsibility for the request. This official need not be a prosecutor. A Fifth Circuit decision, considering the Florida electronic surveillance statute, held that allowing the governor to make an application did not violate Section 2516(2) because the purpose of the Federal requirement that the principal prosecuting attorney of a State or political subdivision make an application was not to designate a particular office by name or title, but to assure a centralization of policy, and such an end would be achieved when the State's highest executive made an application. *United States v. Pacheco*, 489 F.2d 554 (5th Cir. 1974), *cert. denied*, —U.S.—, 95 S.Ct. 1558 (1975).

On the other hand, the contention that responsibility must be pinpointed can go too far. Defendants in New York have tried—unsuccessfully—to attack an eavesdropping order for failure to designate the names of the police officers who would actually carry out the interceptions. *People v. Fiorillo*, 63 Misc.2d 480, 311 N.Y.S.2d 574

(Montgomery County Ct. 1970). The court in *Fiorillo* viewed such a procedure as both impractical and unnecessary.

h. Judicial Approval of Electronic Surveillance Order

Title III limits approval of Federal surveillance orders to Judges of United States District Courts or Courts of Appeals. 18 U.S.C. 2510(9). This provision reflects a view that the ordinary Federal search warrant procedures, which allow United States Magistrates to issue warrants, is too permissive for the interception of wire or oral communications. State court judges must also meet the standards of 18 U.S.C. 2510(9), i.e., they must be judges of a court of general criminal jurisdiction. Most State statutes simply authorize any of those State courts having jurisdiction over felony trials to sign an electronic surveillance order. Some State statutes are more specific, however. For example, New Jersey's statute calls for the Chief Justice of the State Supreme Court to periodically designate judges of the Superior Court to receive applications and enter surveillance orders. The Delaware statute, too, calls for the designation of judges. Connecticut's electronic surveillance law requires that any intercept order be approved by a panel of three specially designated Superior Court judges. In Rhode Island, the application must go to the presiding justice of the superior court of competent jurisdiction. The Wisconsin statute specifies that, in those counties having more than one branch of the circuit court, applications must go to the circuit court judge of the lowest-numbered branch having criminal jurisdiction.

The issue of which judges in a state exercise general criminal jurisdiction has been occasionally raised. A Federal decision interpreting a Florida State law held that a State Supreme Court justice could issue orders as a judge of general criminal jurisdiction as defined in 18 U.S.C. 2510(9)(b). *United States v. Pacheco*, 489 F.2d 554 (5th Cir. 1974), *cert. denied*,—U.S.—, 95 S.Ct. 1558 (1975). *See also State v. Siegel*, 13 Md. App. 444, 285 A.2d 671 (1971), *aff'd*, 266 Md. 256, 292 A.2d 86 (1972). Of course, failure of a judge to actually sign a surveillance order requires suppression. *United States v. Ceraso*, 355 F.Supp. 126 (M.D.Pa. 1973).

i. Telephone Company Cooperation

The communication companies have been sensitive to any concern on the part of their subscribers that telephones may be wiretapped, even by law enforcement authorities. In the amicus brief submitted in *Olmstead* by four telephone and telegraph companies, the Supreme Court was urged to protect the exclusive use of a telephone by the parties to a conversation. This position did not change. In 1969, a telephone company refused to follow a Federal District Court order to assist law enforcement officers in carrying out a lawful wiretap. The Ninth Circuit ruled that Title III carries no implicit authority for a court to order a private citizen to aid law enforcement. Application of United States, 427 F.2d 639 (9th Cir. 1970). Consequently, an amendment was added to Section 2518(4) of Title III in 1970, and to the laws of some states (including Arizona, Colorado, Connecticut, Nevada, New Jersey, New Mexico, Virginia, and the District of Columbia), that has generally been referred to as the *directive provision*, for its Title III language states:

> An order authorizing the interception of a wire or oral communication shall, upon request of the applicant, direct that a communication common carrier, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such carrier, landlord, custodian, or person is according to the person whose communications are to be intercepted. Any communication common carrier, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant at the prevailing rates.

Telephone companies have cooperated without objection in those jurisdictions which have adopted directive provisions.

j. Designated Offenses

Section 2516(1) of Title III permits interception orders for a broad list of particularly designated offenses, which were chosen because they were "intrinsically serious" or "characteristic of the operations of organized crime." 1968 *U.S. Code Cong. & Ad. News* 2153, at 2186. National security crimes are included within this listing. Section 2516(2) designates offenses for which State laws can authorize electronic surveillance. States can designate crimes of murder, kidnapping, gambling, robbery, bribery, extortion, dealing in dangerous drugs, and other crimes dangerous to life, limb, or property and punishable by imprisonment for more than one year. Conspiracy to commit any of these designated offenses is also included. Most State laws list offenses equivalent to the broad range of Federal crimes designated in Section 2516(1) of Title III. Some states, e.g., Massachusetts, Minnesota, Georgia, and New York, add prostitution to this crimes list. Delaware authorizes interceptions for any felony and Maryland for any crime.

Section 2517(5) of Title III provides that if, in the course of a lawful interception, evidence of of-

fenses other than those specified in the surveillance order is obtained, it may be used in a prosecution if a subsequent application is made to a judge who finds that in all other respects the intercept was carried out in accordance with Title III provisions. The Tenth Circuit dismissed a constitutional challenge to this section, upholding the government's argument that it was analogous to the plain view doctrine admitting unanticipated evidence discovered in physical searches. *United States v. Cox*, 449 F.2d 679 (10th Cir. 1971), *cert. denied*, 406 U.S. 934 (1972). The provision requires that the application to the judge be made as soon as practicable. But a delay in obtaining an order authorizing the admission of evidence for new offenses does not require suppression of evidence gathered in accord with the original order, because the amendment is irrelevant to an ascertainment of the legality of the original order. *United States. v. Denisio*, 360 F.Supp. 715 (D.Md. 1973).

The electronic surveillance statute in New York State has a similar provision but requires amendment of the original electronic surveillance order. New York Code of Crim. Procedure §700.65.4 (McKinney 1973). The statute authorizes the use as evidence of information "not otherwise sought" which is obtained in the course of an authorized intercept, provided that an application for amendment of the original order is sought from a judge as soon as is practicable. Under this provision a New York intermediate appellate court reversed the conviction of a defendant found guilty of conspiracy and attempted robbery, finding that the continued interception of incriminating conversations not included in the order during an 11-day delay in obtaining an amendment did not comply with the statute. *People v. DiStefano*, 45 App. Div. 2d 56, 356 N.Y.S.2d 316 (App. Div. 1974).

k. Specification of Person to be overheard

Section 2518(1)(b) requires, *inter alia*, that the application and order establish "the identity of the person, if known, committing the offense and whose communications are to be intercepted." The Supreme Court has held that individuals must be named in an application or order only if there is probable cause to believe that they are committing the offense for which the wiretap is sought. Furthermore, once the necessity for the intercept has been shown, there is no requirement that the government exhaust traditional investigative methods in an effort to determine the possible complicity of all other persons who may be using the subject telephone. *United States v. Kahn*, 415 U.S. 143 (1974). But the Sixth Circuit has recently held that an omission from the application of names of known persons against whom there is probable cause would require suppression, no matter whether the omission is inadvertent or purposeful. *United States v. Donovan*, 513 F.2d 337 (6th Cir. 1975). Identification of a known suspect has been held to be a precondition of granting of an order. This requirement was cast as important to the exercise of executive approval, prior judicial authorization, subsequent judicial review of interceptions, and compliance with the inventory notice requirement. *United States v. Bernstein*, 509 F.2d 996 (4th Cir. 1975).

l. Amendment of Orders

Although Title III does not have an explicit amendment provision, it does include Section 2517(5) (see 2-j, above) requiring subsequent authorization when unanticipated criminal activity is intercepted. It would seem that Section 2517(5) is primarily directed towards a retrospective analysis of the scope of a court-ordered interception after it has been completed, with judgments made as to the propriety of its breadth and the propriety of the seizure of unrelated criminality. Nevertheless, there is some case law, primarily arising in jurisdictions familiar with the New York amendment procedure, suggesting that more extensive amendment provisions are to be inferred from Title III, although the procedures have not been clearly defined. *See, e.g., United States v. Tortorello*, 480 F.2d 764 (2d Cir. 1973), *cert. denied*, 414 U.S. 866 (1973). The Second Circuit has excluded conversations of a party not named in the original order when the interceptions continued for 17 days after the identity of that person was discovered and the order was not amended. *United States v. Capra*, 501 F.2d 267 (2d Cir. 1974), *cert. denied*, 420 U.S. 990 (1975). However, the majority of the Supreme Court in *Kahn* did not discuss any amendment requirement when such an intercept continued for four days, although three dissenting Justices indicated their belief that there was sufficient time to obtain a broader warrant.

m. Alternative Investigative Means

Section 2518(1)(c) of Title III requires that an application contain a full and complete statement on the previous use of, or reasons for not using, other investigative methods and an explanation why future use of such methods would fail or be too dangerous. This requirement reflects the English wiretap procedure in existence when the statute was passed. 1968 *U.S. Code Cong. & Ad. News*, 2153, at 2190. The kind of normal investigative procedures that should be found to be inadequate before a wiretap order is approved includes stan-

dard surveillance techniques, questioning under grant of immunity, use of search warrants, and infiltration of conspiratorial groups by agents or informants. *Id.* This requirement, that the application show that such techniques reasonably appear unlikely to succeed if tried, is to be reviewed "in a practical and commonsense fashion," and courts have not generally granted motions to suppress on the grounds that the application was deficient in this respect. *United States v. Armocida*, 515 F.2d 29 (3d Cir. 1975); *United States v. James*, 494 F.2d 1007 (D.C.Cir. 1974), *cert. denied*, 419 U.S. 1020 (1974). Several recent decisions, however, indicate a greater judicial concern with this provision. The Ninth Circuit has cautioned that boilerplate recitation of the difficulties of gathering usable evidence is not sufficient. *United States v. Kerrigan*, 514 F.2d 35 (9th Cir. 1975). More recently, the same court held that a motion to suppress wiretap evidence under Section 2518(1)(c) should have been granted. The court found that the wiretap application lacked sufficient factual basis to allow for an independent judgment by the authorizing judge; recitation of the applicant's prior experience of difficulty in investigating the type of crime involved was not sufficient to demonstrate to the authorizing judge that traditional methods either had been unsuccessful or were too dangerous or unlikely to succeed under the particular circumstances of the case. *United States v. Kalustian*, No. 74-3314, 17 Crim. L.Rep. 2428 (9th Cir., Aug. 4, 1975). Another court, in suppressing such evidence, noted that a judge could not use the doctrine of judicial notice to fill in these facts when an application was deficiently drawn. *United States v. Curreri*, 388 F.Supp. 607 (D.Md. 1974).

n. Period of Interception

Federal law allows a maximum of 30-day period of surveillance for an original interception order and for each extension. The number of court-approved extensions that may be obtained upon a showing of probable cause is unlimited under the Federal law. Many Federal orders, however, authorize lesser time periods. Eight states provide for time periods less than the Federal 30-day provision: Connecticut, Kansas, Minnesota, and New Hampshire limit original orders to 10 days; Massachusetts, Virginia and Washington have a 15-day provision; Georgia permits electronic surveillance for a period of 20 days. The Oregon statute initially authorized a longer time period, allowing up to 60 days of interception in the original order, but presumably it is now limited to the 30 days permitted by Federal law. New Jersey, by a very recent amendment to its statute, has a 20-day limit for the original order and allows only two 10-day extensions. Some other states also place a limit on the number of extensions that may be authorized. For example, Colorado allows only one 30-day extension, Connecticut allows a maximum of three 10-day extensions; and Georgia and Washington, by the language of their statutes, appear to authorize only one extension of the original order.

o. Minimization of Interception

Minimization of the interception of non-criminal conversations is required by Section 2518(5) of Title III and similar provisions in State statutes. This practice is a prerequisite to keeping court-authorized electronic surveillance within the bounds of constitutionality as prescribed by the *Berger* decision. The question of what constitutes proper minimization has been perhaps the most difficult of the issues with which the courts have grappled. Each case demands a close examination of the facts of execution of the surveillance order. Minimization has not yet been the subject of a post-Title III Supreme Court opinion. The present definitive judicial statement on the issue may be found in *United States v. Bynum*, 360 F.Supp. 400 (S.D.N.Y. 1973), and the Second Circuit decision in the same case approving and adopting the findings of the District Court. 485 F.2d 490 (2d Cir. 1973), *vacated on other grounds*, 417 U.S. 903 (1974). The opinions note that minimization is satisfied if "the court on review of the government's procedures concludes, in the light of all facts and circumstances of the case, that 'on the whole the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion.'" 360 F.Supp. at 409. Reasonableness is a factual question, requiring a case-by-case analysis, with a number of constituent factors to be included. 360 F.Supp. at 410. The Court of Appeals notes that the mere fact that every conversation is monitored does not necessarily violate the statutory minimization procedure. There is no "hard and fast" formula to determine what law enforcement agents could anticipate in detecting any pattern of innocent conversations during surveillance. 485 F.2d at 500. The court recited all the screening procedures used in the case and concluded that they were the best possible under the circumstances. Particular attention is given to the degree of judicial supervision in determining whether a good faith minimization effort was attempted. 485 F.2d at 501. Other factors to be considered include the nature and scope of the criminal enterprise under investigation, and the government's reasonable expectation as to the character of the conversations. *United States v. Tor-*

torello, 480 F.2d 764 (2d Cir. 1973), *cert. denied*, 414 U.S. 866 (1973); *United States v. Armocida*, 515 F.2d 29 (3rd Cir. 1975); *United States v. James*, 494 F.2d 1007 (D.C.Cir. 1974), *cert. denied*, 419 U.S. 1020 (1974).

Other Federal appellate courts have since employed the minimization analysis of *Bynum*. *See, e.g., United States v. John*, 508 F.2d 1134 (8th Cir. 1975); *United States v. Quintana*, 508 F.2d 867 (7th Cir. 1975); *United States v. Scott*, 504 F.2d 194 (D.C.Cir. 1974). One court has noted that demonstration of the reasonableness of the screening procedures actually employed by government agents shifts to the defendants the burden of showing what other procedures would better have minimized interception of noncriminal conversations while still permitting the government to achieve its legitimate objectives. *United States v. Quintana*, *supra*.

Federal officers executing surveillance orders must be instructed not to intercept conversations that are protected by evidentiary privileges. Section 2517(4) provides that otherwise privileged conversations that are intercepted do not lose their privileged character. Some states, e.g., Delaware and New Jersey, require a showing of "special need" before an order may be issued to tap the telephone of a privileged party, such as a clergyman or an attorney. In addition to protecting traditionally privileged conversations (lawyer-client, physician-patient, etc.) New Jersey has extended its requirement of "special need" to the telephones of psychologists and reporters. The Connecticut statute totally bars issuance of any wiretap order on the telephone of any physician, attorney or clergyman. This is not to say, however, that an otherwise privileged conversation may not lose its privilege if it involves criminal activity. *See American Bar Association Standards on Electronic Surveillance*, Approved Draft, 1971, pp. 152-158.

p. Automatic Termination of Interception

In accordance with the constitutional prerequisite of particularity of searches, Section 2518(4)(e) of Title III, and similarly worded sections of State laws, provide that every order shall specify "the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained." Courts have reached differing conclusions on failure to include a statement concerning automatic termination in surveillance orders. Section 2518(4)(e), according to *United States v. Cafero*, 473 F.2d 489 (3d Cir. 1973), *cert. denied*, 417 U.S. 918 (1974), must be interpreted in light of Section 2518(5), providing that no interception may go on longer than necessary. Further, Section 2518(5) must be read "as requiring automatic termination upon attainment of the objective of the authorization irrespective of whether a statement to this effect has been included by the authorizing judge." 473 F.2d at 496 (dicta). It would seem, therefore, that absence of any clause dealing with termination of a wiretap order would simply mean that the order terminates automatically on the first relevant interception. Of course the court may avoid this automatic termination, pursuant to Section 2518(4)(e), by explicitly authorizing the interception to continue beyond the first attainment of its objective.

But several State Courts dealing with the issue have viewed the absence of a clause concerning termination as rendering the order void on its face and requiring automatic suppression. *Johnson v. State*, 226 Ga. 805, 177 S.E.2d 699 (1970); *State v. Siegel*, 266 Md. 256, 292 A.2d 86 (1972); *People v. Pieri*, 69 Misc. 2d 1085, 332 N.Y.S.2d 786 (Erie County Ct. 1972), *aff'd*, 346 N.Y.S.2d 213 (App.Div. 1973); *People v. Botta*, 60 Misc.2d 869, 304 N.Y.S.2d 362 (Nassau County Dist. Ct. 1969). On the other hand, the Second Circuit in *United States v. Poeta*, 455 F.2d 117 (2d Cir. 1972), *cert. denied*, 406 U.S. 948 (1972), ruled that an inadvertent exclusion of a paragraph authorizing interception beyond the first incriminating conversation would not be a ground for suppression when the rationale behind the continuous interception was apparent from affidavits used in the application; substantial compliance with Section 2518(4)(e) had thereby been achieved. This position was also followed in *United States v. Carubia*, 377 F.Supp. 1099 (E.D.N.Y. 1974).

q. Additional Limitations on Issuance of Electronic Surveillance Orders

Some State legislatures have placed additional types of procedural limitations on authorizations for nonconsensual electronic surveillance as particular problems are encountered with use of the investigative technique in that State. For example, New Jersey requires that an applicant show special need for surveillance over a public telephone (N.J. Stat Ann. §2A: 156A-11(1973 Supp.)), and New York requires a court order for entry into a building for the installation of a bug (New York Code of Crim. Procedure § 700.30.8) (McKinney 1973). Connecticut, which has highly restrictive procedures for obtaining a court order, has adopted an ultimate limit (35) to the number of orders which may be granted annually in the state (Connecticut General Statutes Annotated, §54-41d(9)).

r. Sealing and Custody of Records

Both tape recordings of interceptions and actual applications and orders must be treated confidentially, subject to sealing and judicial custodial control, pursuant to Section 2518(8) of Title III and similar State statutues. Judges may use their contempt powers to enforce these provisions. Substantial compliance with these provisions is all that is required. *United States v. Cantor*, 470 F.2d 890 (3d Cir. 1972). In a more recent Third Circuit case the court concluded that the sealing requirement's purpose is to maintain the integrity of tapes for evidentiary purposes and not to limit the use of interception procedures. Thus a failure to seal promptly does not render a communication "unlawfully intercepted" and does not necessitate suppression under the statute. *United States v. Falcone*, 505 F.2d 478 (3rd Cir. 1974), *cert. denied*, 420 U.S. 955 (1975). But a District Court in Michigan has reached a different conclusion, granting a motion to exclude tape recordings which were not sealed in accordance with the provisions of Title III. The court held that the procedures in the act were intended to protect the Fourth Amendment rights of the individual and must therefore be strictly construed. *United States v. Lucido*, No. 49234 (E.D.Mich., Sept. 4, 1974). A New York court, in construing a requirement of immediate delivery of recorded conversations to the judge who authorized interception, concluded that a three-day delay, under the facts of the case, nevertheless complied with the statute; the court noted that the word "immediately" does not mean "instantaneously." *People v. Blanda*, 80 Misc.2d 79, 362 N.Y.S.2d 735 (Monroe County Sup. Ct. 1974). This decision, however, followed an earlier ruling calling for strict construction of the sealing requirement. *People v. Nicoletti*, 34 N.Y.2d 249, 313 N.E.2d 336, 356 N.Y.S.2d 855 (1974). In *Nicoletti*, suppression was decreed because tape recordings of intercepted conversations were held for a month after the end of interception and then delivered to the District Attorney, but not to the judge who authorized interception. A Florida Federal court refused to suppress all tapes when some tapes had not been properly sealed, observing that no prejudice resulted to defendants because unsealed tapes had not actually been introduced into evidence. *United States v. Lanza*, 349 F.Supp. 929 (M.D.Fla. 1972).

s. Notice of Interception

Subparagraph 2518(8)(d) of Title III, reflecting ordinary search warrant procedure, requires the judge issuing the order to cause the law enforcement agency executing the order to serve an inventory on the person named in the order within 90 days after interception is terminated. The inventory must contain a notice of the entry of the surveillance order, the date of the entry, the period of authorized interception, and a specification of whether oral or wire communications were or were not intercepted. The lack of such a provision was one of the reasons the New York statute considered in *Berger* was found to be unconstitutional. The notice provision of Title III has been deemed an absolutely necessary link in the chain of protective measures built into the statute. *United States v. Eastman*, 326 F.Supp. 1038 (M.D.Pa. 1971) *aff'd* 465 F.2d 1057 (1972). See, similarly, under New York law, *People v. Hueston*, 34 N.Y.2d 116, 312 N.E.2d 462, 356 N.Y.S.2d 272 (1974), *cert. denied*,—U.S.—, 95 S.Ct. 1676 (1975). This notice procedure also serves the purpose of implementing the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary device. *United States v. Donovan*, 513 F.2d 337 (6th Cir. 1975).

Service of inventory notice to parties to intercepted conversations who are not named in the order is discretionary with the judge issuing the surveillance order. The presence of such discretion was criticized in the *Whitaker* decision, 343 F.Supp 358 (E.D.Pa. 1972), the one case to date finding Title III to be unconstitutional, which was later reversed by the Third Circuit. 474 F.2d 1246 (3d Cir. 1973), *cert. denied*, 412 U.S. 953 (1973). One Federal Court has stated that any weakness in the statute due to the artificial distinction between named persons and others whose communications have been intercepted, is cured by Section 2518(9), which requires a copy of the order and application to be served upon a party against whom it is to be used ten days prior to any proceeding. *United States v. Ripka*, 349 F.Supp. 539 (E.D.Pa. 1972), *aff'd*, 480 F.2d 919 (3rd Cir. 1973), *cert. denied*, 414 U.S. 979 (1974). More recent cases have held that the prosecution is required to transmit to the authorizing judge information regarding all those whose conversations have been intercepted, regardless of whether they are named in the order, in order to give the judge adequate opportunity to exercise his discretion in determining who should receive notice. *United States v. Chun*, 503 F.2d 533 (9th Cir. 1974); *United States v. Donovan*, 513 F.2d 337 (6th Cir. 1975).

Distinctions on whether failure to provide formal or timely notice must lead to suppression seem to be based on the possibilities of prejudice. The Eighth Circuit has held that defendants who received actual notice of surveillance were not

prejudiced by failure to receive a formal inventory, and could not prevail on a suppression motion. *United States v. Wolk*, 466 F.2d 1143 (8th Cir. 1972). The New York Court of Appeals held that if actual knowledge of the existence of the order is demonstrated within the time period allowed for notification by the prosecution, a formal written notification becomes a ministerial act and the failure to give formal notice does not require suppression of evidence. *People v. Hueston*, *supra*. Similarly, when failure to make service of the inventory within the statutory time limits is inadvertent and not chargeable to the bad faith of prosecutors, and defendants suffer no prejudice thereby, suppression will not be granted. *State v. Dye*, 60 N.J. 518, 291 A.2d 825 (1972), *cert. denied*, 409 U.S. 1090 (1972). A Federal court did not require suppression when a 60-day postponement was received two days after expiration of the initial 90-day time period, and inventories were served more than a month after the expiration day of the 60-day extension of the authorized interception; the court ruled that the delay had resulted from mere oversight and not from intentional governmental abuse. *United States v. Lucido*, 373 F.Supp. 1142 (E.D.Mich. 1974). A nine-day delay in filing of the inventory notice due to clerical mistakes was ruled an insufficient ground for granting a suppression motion. *United States v. LaGorga*, 336 F.Supp. 190 (W.D.Pa. 1971).

On the other hand, failure to provide notice to defendants, although many other persons known to defendants received notice, led the Sixth Circuit to affirm the grant of a motion to suppress. *United States v. Donovan*, 513 F.2d 337 (6th Cir. 1975). A Florida intermediate appellate court affirmed the grant of a suppression motion when the inventory was not served until eight months after the intercept, declaring that permission to postpone service of the inventory does not give authority to extend the time period for an indefinite duration. *State v. Berjah*, 226 So.2d 696 (Fla.Dist.Ct.App. 1972). A statute recently enacted in Florida offers further protection to the victims of electronic surveillance by prohibiting publication or broadcast of the name of any individual served with notice of interception until that person has been formally indicted or informed against. Florida Statutes Annotated §934.091 (1974).

t. Discovery

The discovery provisions of Title III are found in Section 2518(8)(d):

> . . . The judge, upon the filing of a motion, may in his discretion make available to such person (given notice of the interception) or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice.

Further, the statute provides for full discovery of the application and order before any evidence derived therefrom can be introduced against a party at any trial, hearing or other proceeding in a Federal or State court. Section 2518(9). These provisions are often joined to the pre-trial discovery procedures specified in Rule 16 of the Federal Rules of Criminal Procedure.

Discovery in criminal trials is allowed at the discretion of the court and must be timely; discovery sought in the midst of trial may be untimely. *United States v. Newman*, 476 F.2d 733 (3d Cir. 1973). But in accordance with the special provisions of the wiretap statute, many rulings arise well before trial; for example, key rulings have been made in the context of grand jury proceedings where persons called as witnesses allege that questions being propounded are derived from illegal surveillance. The issues may also arise after a criminal conviction and, of course, issues concerning discovery of electronic surveillance materials have also arisen in civil damage actions.

The extensive discovery provisions of the electronic surveillance statute are affected by another Federal statutory provision, 18 U.S.C. 3504:

> §3504. Litigation concerning sources of evidence.
>
> (a) In any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body or other authority of the United States—
>
> (1) upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act.
>
> (b) As used in this section "unlawful act" means . . . the use of any electronic, mechanical, or other device (as defined in Section 2510(5) of this title) in violation of the Constitution or laws of the United States or any regulation or standard promulgated thereto.

These broad provisions, though they had their underpinnings in prior case law (see *Alderman v. United States*, 394 U.S. 165 (1969)), have served to extend discovery rights when electronic surveillance is involved. Thus, in *Gelbard v. United States*, 408 U.S. 41 (1972), the Supreme Court held that grand jury proceedings could be interrupted by a witness' refusal to testify on a showing that the questions posed were based on improper electronic surveillance; the showing of such impropriety was discoverable under the provision of Section 3504 of the electronic surveillance statute. The Supreme Court subsequently made it clear that grand jury witnesses had no such rights to challenge questions generally; the right came about in electronic surveillance cases only as a result of the special remedies conferred in Title III. *Calandra v. United States*, 414 U.S. 338 (1974). Nor have courts been prone to expand this special remedy, in the context

of its potential disruption of grand jury inquiries. Thus, a recent First Circuit opinion, finding the government's simple denial of electronic surveillance of a grand jury witness to be sufficient, stated that the *Calandra* decision could be construed as foreclosing the broad inquiry into related taps sought by the defendant. *In Re Mintzer*, 511 F.2d 471 (1st Cir. 1974).

There are other limits, of course, to these seemingly broad statutory discovery provisions. To begin with, only persons given notice that they were overheard or persons against whom some legal proceedings have commenced are in a position to take advantage of these provisions. Further, the government need not necessarily respond automatically once any claim is presented.

Courts have had some difficulties in determining the degree of the initial showing a party to a proceeding must make in order to require an answer by the government concerning whether electronic surveillance has affected the proceeding. The D.C. Circuit had, in *In re Evans*, 452 F.2d 1239 (1971), *cert. denied*, 408 U.S. 930 (1972), decided that the government obligation to comply with the statute arose by a mere assertion that unlawful wiretapping had been used against a party. The Second Circuit followed *Evans* in *United States v. Toscanino*, 500 F.2d 267 (2d Cir. 1974). However, the Ninth Circuit in *United States v. Alter*, 482 F.2d 1016 (1973), decided that the statutory duty arose only after the aggrieved person made a *prima facie* case that such surveillance had occurred and that a mere claim of such surveillance was insufficient. But later, the Ninth Circuit, in *United States v. Vielguth*, 502 F.2d 1257 (1974), seemed to limit its *Alter* holding to a situation in which a party claims that questions put to him are tainted by unlawful surveillance of conversations in which he did not participate; a recalcitrant witness who asserted that he had been a victim of illegal surveillance, citing places and dates, could trigger the Government's duty to respond under 18 U.S.C. 3504.

Another intricate issue is that of determining the degree of relevance of an alleged electronic surveillance to the proceedings at hand. If a defendant at a criminal trial has alleged the existence of illegal electronic surveillance, and the government has admitted the truth of some of these allegations, a hearing is necessary to determine the effect of such surveillance, but the timing of the hearing is at the discretion of the trial judge. *United States v. McCarthy*, 292 F.Supp. 937 (S.D.N.Y. 1968). Further, even when illegal electronic surveillance has no apparent relevance to a conviction, a defendant does have a right to an adversary hearing to demonstrate any connection between illegal electronic surveillance and his conviction. *United States v. Fox*, 455 F.2d 131 (5th Cir. 1972). But it appears that the defendant must first demonstrate at least a remote possibility that electronic surveillance could have resulted in tainted evidence. *United States v. Sellers*, 315 F.Supp. 1022 (N.D.Ga. 1970).

Defendants charged with contempt for their trial conduct who made a motion for disclosure of any Federal, State, local, or private electronic surveillance could not prevail because there is no recognizable problem of taint. However, if such evidence is in fact used at the trial, a motion for a taint hearing may be maintained at or after the trial. *In re Dellinger*, 357 F.Supp. 949 (N.D.Ill. 1973).

Once the potential effect on the proceedings is established, the courts must consider the adequacy of the government's response. Several recent decisions have held that when a defendant raises a general claim, under Section 3504, that he was subjected to electronic surveillance, and the claim is not supported by facts, the government denial may be one of a general nature. *United States v. Stevens*, 510 F.2d 1101 (5th Cir. 1975); *United States v. See*, 505 F.2d 845 (9th Cir. 1974), *cert. denied*, —U.S.—, 95 S.Ct. 1428 (1975); *United States v. D'Andrea*, 495 F.2d 1170 (3rd Cir. 1974), *cert. denied*, 419 U.S. 855 (1974). However, once previous government indiscretions have been made known in a case, the form of the denial of illegal surveillance must be an affidavit by a responsible government official. *Korman v. United States*, 486 F.2d 926 (7th Cir. 1973).

If a taint hearing is held and it is determined that the government has violated Section 2518(8)(a) by destroying tapes of illegal surveillance, a grand jury witness' contempt conviction will be reversed, as the government cannot compel a party who objects to unlawful electronic surveillance to go forward with a showing of the taint and then withhold the means to meet that burden. *United States v. Huss*, 482 F.2d 38 (2d Cir. 1973). But a defendant in a burglary conspiracy trial who had been overheard on a national security foreign intelligence tap could not obtain discovery and inspect the tapes after an *in camera* inspection showed the tapes had no connection to the criminal charges. *United States v. Lemonakis*, 485 F.2d 941 (D.C.Cir. 1973), *cert. denied*, 415 U.S. 989 (1974). In a civil suit charging the government with excessive surveillance, where defendants moved to compel divulgence of government surveillance, records and procedures, the Federal court for the Eastern District of Pennsylvania ruled that the government must list the date, time, and duration of conversations overheard during warrantless national security electronic surveillance, but the government can withhold information by invoking a claim of privilege, with the court

to determine the extent to which the need of the party moving for disclosure outweighs the claim of privilege. *Philadelphia Resistance v. Mitchell*, 58 F.R.D. 139 (E.D.Pa. 1972). The same result was reached in a recent decision by another district court. The court recognized the governmental privilege established in *United States v. Reynolds*, 345 U.S. 1 (1953), which protects absolutely secrets of state and military secrets, but held that the assertion of this privilege must be made in such a way that the court can determine whether the government's need for secrecy outweighs the plaintiff's need for the evidence. Under the rule in *Reynolds*, the head of the department or agency responsible for the information must personally assert the privilege with enough particularity to enable the court to make an informed decision. *Kinoy v. Mitchell*, —F.Supp.—, 17 Crim.L.Rep. 2278 (S.D.N.Y. June 3, 1975). *See also Jabara v. Kelly*, 62 F.R.D. 424 (E.D.Mich. 1974); *Frankenhausen v. Rizzo*, 59 F.R.D. 339 (E.D.Pa. 1973).

Considering the problem as a whole, the New York Court of Appeals has suggested a procedure, based on decisions of federal courts, to deal with claims concerning the source of evidence: (1) a specification of the facts leading a defendant to believe that illegal electronic surveillance has taken place, including a listing of the dates of suspected surveillance, the telephone numbers where conversations might have been intercepted, the identity of persons believed to be under surveillance, and an explanation of how the surveillance could be linked to the legal proceeding in which the claim is brought; (2) upon such a sufficient showing the state must affirm or deny such allegations, ordinarily by an affidavit alleging facts supporting a denial of the claim, signed by the District Attorney or his designate; (3) this affidavit should state what steps have been taken, the persons and agencies contacted about electronic surveillance, and the substance of inquiries that were made, including the dates of claimed surveillance to which inquiries were addressed; (4) the court shall then determine if a hearing shall be conducted concerning the claim. *People v. Cruz*, 34 N.Y.2d 362, 314 N.E.2d 39, 357 N.Y.S.2d 709 (1974), *modified*, 35 N.Y.2d 708, 320 N.E.2d 274, 361 N.Y.S.2d 641 (1974).

u. Exclusionary Rule and Suppression of Evidence

Once it is clear that evidence deriving from electronic surveillance has been or is intended to be used against a party in a legal proceeding, the issue becomes one of suppression of evidence. When a criminal prosecution is based on electronic surveillance evidence, the motion to suppress evidence usually becomes the focal point of the trial. Section 2515 of Title III prohibits the use of any evidence obtained in violation of the electronic surveillance law in any legal proceeding.

(1) Standing to bring the motion

In *Alderman v. United States*, 394 U.S. 165 (1969), the Supreme Court held that persons with standing were entitled to a suppression hearing to determine if electronic surveillance conducted by the Government had been in violation of the Fourth Amendment. Persons with "standing" were defined as those who had their conversations intercepted or whose premises had been invaded during the illegal surveillance. Although the three consolidated cases in *Alderman* involved surveillance undertaken before Title III was enacted, the Court cited Title III's definition of "aggrieved person" and its provision of a suppression remedy, noting that these were legislative restatements of prior case law.

Section 2510(11) of Title III defines an "aggrieved person," who can move to suppress, as "a person who was a party to an intercepted wire or oral communication or a person against whom the interception was directed." The legislative history to Section 1510(11) notes that this definition of "aggrieved person" was intended to reflect the case law (*see also Alderman v. United States*, 394 U.S. 165, 175 n.9 (1969)). The provision was not intended as a departure from Rule 41(e) of the Federal Rules of Criminal Procedure. *United States v. King*, 478 F.2d 494 (9th Cir. 1973), *cert. denied*, 417 U.S. 920 (1974). Thus, illegal electronic surveillance of one member of a group does not make others in the group who are charged with a conspiracy aggrieved persons within the meaning of the statute. However, all parties who are actually intercepted have standing to move to suppress. *United States v. Ahmad*, 347 F.Supp. 912 (M.D.Pa. 1972). And a defendant who was overheard on a subsequent wiretap in an investigation can attack the legality of an earlier source wiretap and obtain suppression. *People v. Brown*. —Misc.2d—, 364 N.Y.S.2d 364 (Sup. Ct. 1975). A suppression motion must, however, be made before trial or it may be waived. *Sisca v. United States*, 503 F.2d 1337 (2d Cir. 1974), *cert. denied*, 419 U.S. 1008 (1974).

The Supreme Court extended the suppression remedy of Section 2515 in *Gelbard v. United States*, 408 U.S. 41 (1972), holding that a grand jury witness held in civil contempt for a refusal to testify could invoke 18 U.S.C. 2515 as a defense if the grand jury's questions were based on illegal surveillance, but this extension has been somewhat limited. For example, the First Circuit thereafter held that a suppression hearing was unavailable to a grand jury witness not held in contempt. *Cali v. United States*, 464 F.2d 475 (1st Cir. 1972). The

First Circuit also held that the remedy was unavailable at least at this stage, if a wiretap order was not facially defective *In re Marcus*, 491 F.2d 901 (1st Cir. 1974), *vacated on other grounds*, 417 U.S. 942 (1974). Nor, of course, was it available with relation to evidence obtained by a wired agent, since Title III allows consensual recording *United States v. Friedland*, 444 F.2d 710 (1st Cir. 1971).

In *Calandra v. United States*, 414 U.S. 338 (1974), the constitutional rule excluding unlawfully seized evidence was held to be inapplicable to grand jury proceedings. However, the Court noted that this finding did not affect electronic surveillance evidence because the remedy of suppression of illegally obtained electronic surveillance evidence was statutory and went beyond constitutional requirements.

(2) Scope of the remedy.

Section 2515 of the electronic surveillance statute excludes the use of any evidence derived from electronic surveillance conducted in violation of Title III. The grounds for a motion to suppress such evidence are set forth in Section 2518(10)(a). The grounds are that, (i) the communication was unlawfully intercepted, (ii) the order of authorization or approval is insufficient on its face, or (iii) the interception was not made in conformity with the order.

Concerning the substance of the suppression remedy, the Supreme Court, in the *Giordano* and *Chavez* decisions, made it clear that suppression of the evidence would be mandated by failure to satisfy any of those statutory requirements which directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device. But, in *Chavez*, the misidentification of the officer authorizing the wiretap application when, in fact, the Attorney General had been the person who properly authorized it, was viewed as not affecting the "fulfillment of any of the reviewing or approval functions required by Congress." 416 U.S. at 575. The four justices who dissented in *Chavez* believed that a fair reading of Title III would not authorize courts to "pick and choose among various statutory provisions, suppressing evidence only when they determine that a provision is 'substantive,' 'central,' or 'directly' and 'substantially' related to the congressional scheme." 416 U.S. at 585-86. But this is exactly what the courts have been doing, since the *Giordano* and *Chavez* decisions, with respect to the host of procedural problems discussed above. For example, the issues as to whether the lack of alternative investigative means has been properly set forth (Section *m*, *supra*), and whether adequate notice had been provided to the subjects of electronic surveillance (Section *s*, above), have received especially close scrutiny of late.

A key issue in considering the scope of the suppression remedy concerns minimization. The puzzling question has been whether, on a finding that interceptions have not been properly minimized in accordance with statutory requirements, all intercepted conversations or only those beyond proper minimization standards must be suppressed. In ordering suppression, the Federal and State courts have generally adopted a rule that the remedy will be applied to interceptions found to be unlawful and not to all intercepted conversations, unless the minimization requirements have been blatently ignored, in which case all evidence obtained in the electronic surveillance will be suppressed. *United States v. Mainello*, 345 F.Supp. 863 (E.D.N.Y. 1972); *United States v. LaGorga*, 336 F.Supp. 190 (W.D.Pa. 1971); *United States v. Lanza*, 349 F.Supp 929 (M.D.Fla. 1972); *Rodriguez v. State*, 297 So.2d 15 (Fla. 1974); *see also People v. Solomon*, 74 Misc.2d 926, 346 N.Y.S.2d 938 (Kings County Sup. Ct. 1973) (upholding order despite inadvertent failure to include minimization clause in original warrant).

Another problem area has been whether a defect in an original order mandates the suppression of interceptions obtained in extensions or subsequent related surveillance orders based on information derived from a tap under the defective order. The statute (Section 2515), iterating case law, proscribes the use of evidence derived from an unlawful interception. The prevailing rule, therefore, is that if a properly authorized extension is based on probable cause principally derived from information from invalidly authorized taps, it must be suppressed. *United States v. Calallero*, 503 F.2d 1018 (6th Cir. 1974). The legal burden proof in showing that a subsequent application was tainted by the use of information from an earlier illegal interception rests upon the party making the suppression motion. *United States v. Ceraso*, 355 F.Supp. 126 (M.D.Pa. 1973).

(3) Appealablity.

Title III (Section 2518(10)(b)) and some State statutes allow the government to appeal the granting of a motion to suppress. However, the denial of such a motion is not appealable because such a ruling is not a final judgment or order. *United States v. Smith*, 463 F.2d 710 (10th Cir. 1972). New York, however, pursuant to its general rule regarding suppression motions, permits a defendant to appeal from the denial of his motion to suppress evidence even after a plea of guilty to the substantive charge. New York Criminal Procedure Law, §710.70(2).

v. Use of Electronic Surveillance Evidence at Trial: Voice Identification and Transcripts

Tapes of intercepted conversations to be used in evidence must be kept under careful custody, including compliance with the sealing requirement discussed earlier. The voice of the person whose conversations are intercepted must be identified. This is usually done through the testimony of a person who is familiar with the voice to be identified, and through references in the recorded conversations themselves to the person speaking, but more recently the voiceprint—a scientific technique of measuring a recorded voice through spectrogram analysis—has been used in identifying participants in conversations. More and more courts are accepting the validity of voiceprint identifications, though a number of courts which have dealt with the issue still believe that the process is inadequately developed and that its reliability is not yet established. *United States v. Addison*, 498 F.2d 741 (D.C. Cir. 1974); *see also United States v. Franks*, 511 F.2d 25 (6th Cir. 1975) (citing State and Federal decisions to date). The Supreme Judicial Court of Massachusetts has recently held that the technique has received enough acceptance to qualify for prosecutorial use under the "general acceptance in the scientific community" test. *Commonwealth v. Lykus*,—Mass.—, 17 Crim.L.Rep. 2081 (March 27, 1975). Two Circuit courts have also recently admitted voiceprint identification, finding that the dangers inherent in the relatively new scientific technique were minimized by the presentation of the procedures by which the expert reached his opinion. This, combined with exploration of the limitations of the technique on cross-examination, permitted the jury to reach an objective conclusion regarding its reliability. *United States v. Baller*, —F.2d —, 17 Crim.L.Rep. 2359 (4th Cir. July 9, 1975); *United States v. Franks*, *supra*.

The foundation requirement for the use of witness testimony for voice identification is that the identifier has heard the voice at some time. The minimal nature of the identifier's exposure to the voice merely goes to the weight of the evidence. *United States v. Rizzo*, 492 F.2d 443 (2d Cir. 1974), *cert. denied*, 417 U.S. 944 (1974). This requirement is satisfied if the witness has acquired his knowledge of the person's voice after the event testified to by the witness. *United States v. Cox*, 449 F.2d 679 (10th Cir. 1971), *cert. denied*, 406 U.S. 934 (1972). The voice identification at trial of a defendant by a Federal agent who overheard a conversation between the defendant and a government informer wearing a body transmitter has been held not to violate either the due process clause of the Fifth Amendment or the Sixth Amendment's protection of the right to counsel. *United States v. Infelice*, 506 F.2d 1358 (7th Cir. 1974), *cert. denied*, 419 U.S. 1107 (1975), *rehearing denied*, 420 U.S. 956 (1975).

Transcripts of recorded conversations may be used as aids in listening to the recorded conversation. Juries are also permitted to use earphones in listening to tape recorded conversations and this practice is not a denial of the right to public trial. *United States v. Kohne*, 358 F.Supp. 1053 (W.D.Pa. 1973), *aff'd*, 485 F.2d 682 (3d Cir. 1973), *cert. denied*, 417 U.S. 918 (1974).

w. Limitations on Use of Evidence Obtained by Electronic Surveillance in the States

Title III's legislative history indicates that the Federal standards regulating interception of wire or oral communications include a number of constitutional safeguards that must be observed by the states but do not prevent states from enacting stricter laws to protect privacy. As previously noted, while the Federal statute allows consensual recording if one party to a conversation has so agreed, several states make no such allowances or permit electronic recording only after the consent of all parties has been secured.

The major problem, to date, in the disparity between Title III and the law of a state with tighter standards has arisen in the state of California, the most populous state in the nation. The California Supreme Court, for example, has held that a person charged with illegally recording conversations under the State law, which requires the consent of all parties before a conversation can be monitored, could not use the Federal one-party consent standard as a defense in a State prosecution. *People v. Conklin*, 12 Cal.3d 259, 522 P.2d 1049, 114 Cal. Rptr. 241 (1974), dismissed for want of Federal question — U.S. —, 95 S. Ct. 652 (1974). That decision seems non-controversial. But, in a somewhat more dubious decision, of great impact to law enforcement, a California court has held that evidence properly obtained by Federal officers through the use of a wiretap authorized by a Federal judge under Title III could not be received in state criminal proceedings; the court specifically rejected an argument that Title III preempted the more restrictive California wiretap statute. *People v. Jones*, 30 Cal.App.3d 852, 106 Cal. Rptr. 749 (4th Dist. 1973), *dismissed for want of Federal question*, 414 U.S. 804 (1973). The *Jones* ruling should be compared to several rulings by the Ninth Circuit permitting use in Federal courts of evidence obtained by Federal officers using the Federal one-party consent standard in states not ordinarily permitting warrantless one-party consensual eaves-

dropping *United States v. Keen*, 508 F.2d 986 (9th Cir. 1974), *cert. denied*, —U.S.—, 95 S.Ct. 1424 (1975), *United States v. Johnson*, 484 F.2d 165 (9th Cir. 1973), *cert. denied*, 414 U.S. 1112 (1973); *see also United States v. Merritts*, 387 F.Supp. 807 (E.D.Ill. 1975). In *Keen* the court reasoned that the use of such evidence in a Federal court was not prohibited by Title III and was thus governed by Federal common law principle rather than by the particular State statute that would apply to state officers in state courts. Nevertheless, the Ninth Circuit, acting on the basis of the existing California law, has most recently been constrained to hold that a conviction in Federal court, on lawfully obtained Federal wiretap evidence, must be vitiated, because State police officers made the arrest. The arrest, the court reasoned, was unlawful, since California police were not authorized to act on the basis of Federal wiretap information. *United States v. Turner*, —F.2d—, 17 Crim.L.Rep. 2449 (9th Cir. July 24, 1975). The decision illustrates the difficult pass to which Federal-State law enforcement cooperation has been driven by the California rule.

x. Limitation on use of Evidence Obtained by Electronic Surveillance Outside the United States

Application of Title III is ordinarily limited to the United States and its possessions, but when illegal electronic surveillance, with Federal agent participation, takes place overseas, the discovery provisions of 18 U.S.C. 3504 have been held to be available to an alien if there is a potential violation of the Fourth Amendment, and evidence is sought to be admitted in a legal proceeding in the United States. The Fourth Amendment's protection against government directed illegal searches and seizures protects persons, and this protection is not abandoned at international boundaries or limited to those who are citizens. *United States v. Toscanino*, 500 F.2d 267 (2d Cir. 1974).

y. Illegal Eavesdropping—Criminal and Civil Cases

An examination of reported cases, as well as the records of the Department of Justice, indicates that there have been rather few criminal convictions and civil suits concerning unlawful electronic surveillance. However, the courts have made several observations in interpreting the statute during the course of civil and criminal proceedings under it. A very brief outline of some of these rulings follows.

The Federal law extends to intrastate as well as interstate transactions in instruments primarily useful for electronic surveillance, when the transaction affects interstate commerce. *United States v. Reed*, 489 F.2d 917 (6th Cir. 1974). Courts have not yet considered, however, the constitutionality of this broad proscription against electronic surveillance in a case in which there is no clear interstate nexus. 18 U.S.C. 2511(1)(a).

The government's failure to prove how an illegal electronic surveillance device was installed does not prevent a successful prosecution for illegal interception of phone conversations. *United States v. Goldsmith*, 483 F.2d 441 (5th Cir. 1973). But when voices could have been overheard without such a device, a recording of the conversation was held not to justify an indictment for illegal interception of oral communications. *United States v. Carroll*, 337 F.Supp. 1260 (D.D.C. 1971). Further, subsequent disclosure by a person who has recorded a conversation to which he was a party does not violate Title III, does not create a tortious violation of the right to privacy, and thus an action under Section 2520 is not permitted. *Smith v. Cincinnati Post and Times Star*, 475 F.2d 740 (6th Cir. 1973). The use of an extension phone on a privately operated intercommunications system by a store security officer for purposes of investigation was found not to be violative of the statute. The court concluded that the defendant was merely acting as an agent of his employer and, as such, was involved in protecting the rights and property of his employer in the normal course of his employment as authorized by 18 U.S.C. 2511(2)(a)(i). *United States v. Christman*, 375 F.Supp. 1354 (N.D.Cal. 1974).

Courts have disagreed on whether suit can be brought under the statute by a person who was a victim of electronic surveillance by his spouse. In a decision denying a right of action to a woman against her former husband, the Fifth Circuit held that such action was outside the scope of Title III because Congress clearly was interested in controlling organized crime and did not intend to regulate marital and home conflicts. *Simpson v. Simpson*, 490 F.2d 803 (5th Cir. 1974), *cert. denied*, 419 U.S. 897 (1974). A recent District Court case, however, allowed such a cause of action to a husband tapped by his wife and a private detective, distinguishing *Simpson* and finding that "the gross invasion of an individual's privacy by private detective agencies, law firms and other unknown persons" was not outside the statutory proscription. *Remington v. Remington*, 393 F.Supp. 898, 901 (E.D.Pa. 1975). The Supreme Court of Florida suppressed a husband's tapings of his wife's conversations in a marital dissolution proceeding, stating that the husband had no right to invade his wife's right of privacy by undertaking electronic surveillance without a court order. *Markham v. Markham*, 272 So.2d 813 (Fla. 1973). Similarly, the Supreme Court of Nebraska has ruled that recordings made by a wife of her husband's conversations should

have been excluded under the state wiretap statute. The court found that it was immaterial that the interceptions were on the wife's own telephone since she had not been a party to the recorded conversations. *White v. Longo*, 190 Neb. 703, 212 N.W.2d 84 (1973). An Ohio decision, considering the admissibility of a private detective's tapes in a divorce suit relied on *Simpson* in allowing the recorded conversations into evidence; the dissent relied on the *Markham* decision. *Beaber V. Beaber*, 41 Ohio Misc. 95, 322 N.E.2d 910 (Ct. Common Pleas 1974). The Fifth Circuit has refused to extend the marital relation exception it created in *Simpson* to a defendant who had been convicted of illegally wiretapping his former lover, emphasizing the absence of a marital relationship and the absence of any legal theory for the defendant's right to be on the victim's premises. *United States v. Scrimsher*, 493 F.2d 848 (5th Cir. 1974).

The D.C. Circuit, in an order reversing a District Court decision, has apparently interpreted Section 2515, which prohibits use of intercepted communications as evidence, to prohibit such use even in prosecutions for illegal interception unless the consent of the parties whose conversations were overheard is first obtained. *United States v. Liddy and Allen*, No. 73-1020, 12 Crim.L.Rep. 2343 (D.C.Cir. Jan. 19, 1973). The District Court, refusing to find that the intent of Title III was to prohibit enforcement of its own provisions, had ruled that the evidence should be admitted over the protest of the intercepted parties. *United States v. Liddy*, 354 F.Supp. 217 (D.D.C. 1973). Section 2515 cannot be invoked by a defendant charged with illegal wiretapping, however, since such a defendant does not have standing as an "aggrieved person" under Section 2510(11). *United States v. Bragan*, 499 F.2d 1376 (4th Cir. 1974).

z. Telephone Company Monitoring

Although most telephone companies have been hesitant to extend too much aid to law enforcement authorities in installing wiretaps, they have not been loath to use electronic interception to protect their own property. There are several opinions detailing the legal rights of telephone companies to record and monitor conversations in order to protect the telephone system against fraudulent use. A recent Fifth Circuit decision dealt with a conviction of telephone fraud, in which long distance toll charges were evaded through the use of a device known as a "blue box." The phone company had attached a device to record phone numbers dialed from the defendant's home and business and had attached a recorder to identify the person making the calls and record the opening salutation in about 20 unpaid calls. The court held that the Fourth Amendment protects only the content of a telephone conversation and not the fact that a call was placed or that a particular number was dialed. The court further held that Section 2511(2)(a) of Title III clearly permits a telephone company which has reasonable grounds to suspect that its billing procedures are being bypassed to monitor any phone from which it believes that such unbilled calls are being placed. It may use a device to demonstrate the existence of these calls and may record the salutation. Further, the statute allows the telephone company to divulge the existence of these calls. *United States v. Clegg*, 509 F.2d 605 (5th Cir. 1975). Moreover, this practice has been held not to violate Section 605 of the Federal Communications Act (47 U.S.C. 605) which prohibits the unauthorized publication and interception of communications. *United States v. Freeman*, 373 F.Supp. 50 (S.D.Ind. 1974); *United States v. DeLeeuw*, 368 F.Supp. 426 (E.D.Wis. 1974).

The Pennsylvania Superior Court, however, interpreting for the first time a provision of the State electronic surveillance statute which permits monitoring in connection with "the construction, maintenance or operation" of the telephone company, refused to admit evidence of "blue box" fraud obtained by the telephone company. The court found that the methods used by the telephone company, which included monitoring legal as well as illegal conversations and continuing surveillance long after the necessary evidence was gathered, were more intrusive than necessary and thus violated the overriding purpose of the anti-wiretapping law, the protection of individual privacy. *Commonwealth v. Helms*, —Pa.Super.—, 17 Crim.L.Rep. 2367 (Pa. Super. Ct. June 24, 1975).

Faced with the complaints of a subscriber alleging the receipt of harassing phone calls, the telephone company has found itself in the anomalous position of invading the privacy of one subscriber in an attempt to protect the peace of mind of the other. A Texas state court held that the company had the legal right to place a pen register device on the telephone of the alleged wrongdoer at the behest of the complaining subscriber, and that the caller's privacy was not wrongfully invaded. *Jarvis v. Southwestern Bell Telephone Company*, 432 S.W.2d 189 (Tex.Civ.App. 1968).

3. MAJOR ISSUES ON THE LAW OF ELECTRONIC SURVEILLANCE

The question of the constitutionality of the present Federal electronic surveillance legislation and the State laws modelled on it seems to be settled in favor of compliance with the Fourth Amend-

ment, although the Supreme Court has not yet explicitly ruled on the matter. The Court has not yet issued a definitive ruling on minimization; this has been the most pressing open issue concerning use of court-authorized electronic surveillance. The highly controversial issue whether to impose a warrant requirement on foreign security surveillance also remains open for Supreme Court review. It is conceivable that the Supreme Court may choose to deal with the relationship of the Federal and State laws, insofar as evidence obtained by lawful Federal wiretaps has been ruled to be inadmissible in some State courts (e.g., California's *Jones* decision), although, under present law, this appears to be a matter within the proper province of the State courts. But see the rules's effect on Federal decisions (Section 2(w), *supra*). And the Court may decide to again review the issue of whether consensual eavesdrops are subject to Fourth Amendment rules, considering the closeness of the split on the issue in the *White* case. *See*, *People v. Beavers*, 393 Mich. 554, 227 N.W. 2d 511 (1975), *petition for cert. filed*, 17 Crim.L.Rep. 4131 (U.S. July 5, 1975)(No. 75-21), (adopting Justice Harlan's dissent in *White*).

In the lower Federal courts and in the State courts, the major issues concerning court-authorized electronic surveillance have centered around minimization and the suppression remedy. More decisions can certainly be anticipated involving the questions raised by *Giordano* and *Chavez* concerning the extent to which departures from the detailed procedures set forth in the statute require the remedy of suppression. Rulings on minimization, under the prevailing test set forth in *Bynum* must involve case-by-case determination; issues of proper minimization remain the prime stumbling block in the effectuation of court-authorized electronic surveillance.

There have been relatively few appellate decisions concerning the proscriptions against non-consensual electronic surveillance by members of the public, such as private investigators and spouses. Key issues remain concerning the constitutionality of the statute's intrastate jurisdiction over illegal electronic eavesdropping. Other crucial unresolved issues yet to be determined include the extent to which an employer may overhear his employees, a business may surveil its customers, or a family member may overhear other persons in his household. There are some problems concerning the degree of culpability of persons who are unaware that they are not privileged to overhear others in their household or business, and the issue as to what constitutes a device "primarily useful for the purpose of the surreptitious interception of wire or oral communications" remains problematic in some instances, but these latter problems have not stood in the way of enforcement of the statute against major violators.

CHAPTER V

Compendium of Additional Papers and Documents

Summary of Contents

A. Review of Technology

Armer, Paul. Computer technology and surveillance. Computers and people. v. 24 Sept. 1975 : 8–11.

Association for Computing Machinery. Committee on Computers and Public Policy. A problem list of issues concerning computers and public policy. Communications of the ACM, v. 17, Sept. 1974 : 495–503.

Scoville, Herbert Jr. The technology of surveillance. Society v. 12 Mar./Apr., 1975 : 58–63.

U.S. Congress. Senate. Select Committee to Study Governmental Operations with respect to Intelligence Activities Supplementary detailed staff reports on foreign and military intelligence. Book IV, Senate Report No. 94–755. Washington, U.S. Govt. Print. Off., 1976. Intelligence and technology. p. 109–119.

U.S. National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. State of the art of electronic surveillance. Commission studies. Washington, D.C. : U.S. Govt. Print. Off., 1976. pp. 141–157.

B. Civil Liberties Issues and Policy

American Bar Association. Project on Standards for Criminal Justice. Standards relating to electronic surveillance. [Supplement] Washington, 1971. 250 p.

Introduction and Standards with Commentary and dissenting views. p. 1–30.

Colby, William. Secrecy in an open society. The center magazine, v. IX, Mar./Apr. 1976 : 26–38.

Developments in the law—the national security interest and civil liberties. Harvard law review, v. 85, April 1972 : 1244–1285.

Kelley, Clarence D. But so is the right to law and order. Trial, v. 11, Jan./Feb. 1975 : 23, 27, 32.

Scoville, Herbert Jr. Is espionage a necessary instrument for intelligence gathering? Center report, v. IX, Apr. 1976 : 3–5.

Sheridan, Thomas I., III. Electronic intelligence gathering and the omnibus crime control and safe streets act of 1968. Fordham law review, v. 44, Nov. 1975 : 331–354.

Spann, William B., Jr. Removing political influence from Federal law enforcement agencies. American Bar Association journal, v. 61, Oct. 1975 : 1208–1211.

C. United Nations

United Nations. Secretary-General, 1972— (Waldheim). Human rights and scientific and technological developments: uses of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society; report. New York, 1974. 25 p. (United Nations. Document E/CN. 4/1142/Add. 2).
At head of title: United Nations Economic and Social Council.

A. Review of Technology

[From Computers and People for September 1975]

COMPUTER TECHNOLOGY AND SURVEILLANCE

PAUL ARMER, CENTER FOR ADVANCED STUDY IN THE BEHAVIORAL SCIENCES, STANFORD, CALIF.

> "Suppose you were an advisor to the head of the KGB, the Soviet Secret Police. Suppose you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. The system is not to be too obtrusive or obvious. What would be your decision?"

The state-of-the-art of computer technology—or, putting it somewhat more broadly, about information processing technology—is, I think, a most important sub-set of surveillance technology. I do not pretend to know very much about the technology of bugging and wiretapping; so I will not discuss it explicitly. However, I will be talking about the technology of microelectronics—bugging and wiretapping depend on that same technology.

MEASURING RAPID CHANGE

People concerned with rapid change often find it useful to have a yardstick for measuring the amount of change. The concept of "an order of magnitude" is just such a yardstick. As you know, an order of magnitude is a "factor of ten". We can travel by foot at about 5 miles per hour, by automobile at something like 50 miles per hour, and by jet aircraft at about 500 miles per hour. Here we have 5, 50, and 500; each of these modes of transportation differs in speed from the previous one by a "factor of ten" or an "order of magnitude." [1] Thus, the last century has seen a change of two orders of magnitude in transportation speed. The capability of getting around at 50 miles per hour has profoundly affected our way of life. For example, it made the flight to the suburbs possible, and even influenced our culture. As we hear so often, jet travel has shrunk our world tremendously. With the context of two orders of magnitude change in a century before us, let's look at what has been happening with the electronic computer.

THE ELECTRONIC PART OF COMPUTERS: SPEED, SIZE, COST [2]

The speed of the electronic portion of computers has been increasing by an order of magnitude about every four or five years. During the

[1] Adapted from R. W. Hamming, "Intellectual Implications of the Computer Revolution," American Math Monthly, Vol. 70, No. 1, January 1963.

[2] Based on testimony given June 23, 1975, at hearings held jointly by the Subcommittee on Constitutional Rights of the U.S. Senate Judiciary Committee and the Subcommittee on Science and Technology of the Senate Committee on Commerce.

last decade, the size of the electronics has decreased even faster than that—computers are becoming incredibly small. Most importantly, the cost of raw computer power has declined by an order of magnitude every five to six years, and this trend looks like it will continue for at least another decade.

Computers are now being manufactured such that the entire processor fits on a single chip about an eighth of an inch on a side. To make the processor more useful you have to add another chip or two, or three, for memory and for communicating with the outside world. Systems of this kind can be purchased today for less than $100.

In my classes I often hold up such a device and point out to the students that 25 years ago that amount of computing power would have cost more than $1 million and would have occupied several large rooms.

PYRAMID TECHNOLOGY AND SOME OTHER ANALOGIES

Permit me to make another analogy to emphasize this point. It is estimated that the pyramid of Khufu at Giza in Egypt, built in 3000 B.C., required the labor of 100,000 men for 20 years. If the technology of pyramid building had experienced the same increases in speed and decreases in cost as microelectronic technology has over the last 25 years, a similar monument could be built by 20 men in a single year at a cost insignificant enough to make it reasonable as an outlet for many egos. One needs little imagination to picture how Washington, D.C. would look if this were indeed the case.[3]

We have all seen the impact on our society of an increase in the cost of energy by a factor of two or three. What kind of an impact could you expect from an increase, or reduction, of two or three orders of magnitude—that is, a factor of 100, or 1000? I point out that our society runs on information as well as on energy.

Suppose I were able to predict that the cost of an automobile, or of housing, would decrease by a factor of 100 over the next decade? It is quite reasonable to predict that the cost of raw computer power will indeed decrease by a factor of 100 or more in that period of time.

There will be several microprocessors in every car; trucks will probably have one at each end of every axle; there will be one in most appliances, and there will be one pasted on the back of every typewriter. I am sure there are countless uses that we don't even dream of today.

First, I would like to to say a bit about myself so that you can put my comments into context. I think of myself as a "computer-nik." I have been in the computer field since 1947, which was about the time that we began to realize the enormous potentialities of computers for processing information. From 1947 until 1968 I worked at the Rand Corporation, spending ten of those years as head of their computer science department. I am currently a Fellow at the Center for Advanced Study in the Behavioral Sciences, where I coordinate a Program on Science, Technology and Society sponsored by the National Science Foundation.

In 1962 I began to devote time to studying the social implications of information processing technology, and since 1971 that has been my major area of

[3] Adapted from W. H. Davidow, unpublished paper presented at a conference of the Computer Society of the Institute of Electrical and Electronics Engineers, Inc., Washington, D.C., Sept. 10, 1974.

concern. Consequently, I am pleased to be here because the impact of information processing technology on privacy and on freedom has been a concern of mine for more than a decade. I feel that the possible uses of computers for surveillance may not yet be fully recognized.

Other Computer Costs

Lest I leave you with the impression that information processing is about to become a free good, I must emphasize that I am talking only about the electronic portions of computers—there are many other activities associated with making use of a computer. There are mechanical devices for getting information into and out of computers; there are sensors which measure information such as a person's blood pressure or the acceleration of a truck and then feed the information into the computer. Another significant cost is the cost of programing the computer.

Now, the costs of all these other factors are not changing very rapidly, so the total systems' cost is not going to zero; but the cost of the electronics, for all practical purposes, is going to zero.

INFORMATION PROCESSING AND SURVEILLANCE

Now, what does information processing technology have to do with surveillance? A great deal. However, to my knowledge very little information processing technology has been researched and developed as surveillance technology per se; rather, it has been developed with other motives in mind, like improving business data processing or guiding missiles or getting men to the moon. But surveillance is an information processing task just as much as a payroll application is. If you improve the efficiency of information processing technology for payrolls, you improve it for surveillance. Often systems that are put up for other reasons (as we shall see shortly) can also serve surveillance.

NETWORKS

Before going to that, I want to talk about several areas of information processing technology which are of particular importance to surveillance. We have heard quite a bit about networks from Mr. Cooke this morning, due to the publicity given to them of late as though they represented a great new technological breakthrough.

The first networks consisted of many terminals connected to a single computer. Though there may have been earlier examples, I believe that American Airlines' first seat reservation system went into operation about 1952. It soon became clear that one could just as easily communicate from one computer to another as from a terminal to a computer.

INTERFACE MESSAGE PROCESSORS

Now, the most sophisticated computer network that I am aware of is the ARPANET, which was described this morning. It was put up by ARPA—beginning in 1968. The ideas behind the network had been known for at least five years—ARPA put them together in a system for the first time. As Mr. Cooke told you, the network consists of a

number of computers (called "hosts"), communication lines, terminals, and devices called IMPs (for Interface Message Processor). Since there are a number of dissimilar host computers in the network and an even greater variety of terminals, the IMPs must be capable of handling dissimilar host computers and terminals.

It has been said during the last month that "setting up a computer network involving virtually any computer, government or private, is almost as easy as making a telephone call." [4] This statement is dead wrong. First of all, to get into a computer from a network, either the computer must be physically connected to the network, or the network must be able to establish a dial-up connection with the computer.

CONNECTIONS OF COMPUTERS TO COMMUNICATIONS

Most of the computers in operation today are not connected to any communication system. Of the few that are, most are connected to intra-company networks, using lines leased from a common carrier; and/or they may have telephone numbers which can be dialed by a terminal or by another computer. Even if two computers are connected to the same network, unless host-to-host protocols have been agreed to (and adhered to), no IMP will be able to transfer information from one computer to another.

Now, this is not to say that five government agencies couldn't agree on such protocols, and agree to interconnect their computers, and then pass information back and forth. Mr. Cooke described just such a system when he described the COINS network earlier. But the notion that one computer could surreptitiously go around stealing information from any unsuspecting computer, government or private, is hogwash.

PENETRATION OF COMPUTER SYSTEMS

Five or ten years from now most computers will probably be attached to a network, or be reachable via a telephone number. And most will probably adhere to a standard protocol. But by then we should have been wise enough to develop safeguards that will make unwanted penetration from the outside difficult and expensive. Note that I didn't say "impossible".

Even if two computers are connected to the same network and adhere to a common protocol for exchanging messages, the problem of, say, collating together two files on individuals can still be quite difficult. Is Bill Jones the same as William E. Jones? If both records have the same address, it's probably a safe assumption, but if the addresses are different, you don't really know, for the two records may have been obtained at quite different times.

THE UNIVERSAL IDENTIFIER

For this reason those who face the task of putting such files together would like to have a universal identifier: they usually suggest that we use the Social Security number for this universal identifier. Those who fear the results of the collation of several files into complete dossiers

[4] W. Raspberry, Washington Post, June 18, 1975, quoting Ford Rowan of NBC News.

naturally oppose the use of any form of universal identifier. I mention this because I believe it is important that we understand the implications for privacy and surveillance before adopting a universal identifier or permitting the Social Security number to become a universal identifier.

I don't mean to imply that computers today are not penetrated by individuals with malevolent intent. One of the more publicized instances of computer crime involved penetration of a telephone company computer used for supplying equipment and spare parts needed by company employees. The penetrator would dial in, order large amounts of equipment, and have it delivered to a location from which he could subsequently remove it. Over time, he obtained equipment worth several hundred thousands of dollars.

A FAVORITE PASTIME OF BRIGHT STUDENTS

On university campuses a favorite pastime of bright students is to attempt to penetrate the computer. And they succeed all the time.

For the above reasons I believe that those in charge of military security still (with only a few exceptions) will not permit the storage of classified material in a computer which can be accessed from the outside. Thus, if one has personal data files with sensitive information therein, they should be treated like classified material.

Let me say a bit more about security in computer systems. Security was recognized as a problem only recently. As a result there are practically no computers in use today that were designed and built with the security problem in mind. Security precautions that have been incorporated into computer systems are invariably only in the software, or in control of physical access to the computer and terminals. Software is indeed soft. Good security requires that both the hardware and the software be designed with security in mind.

It is interesting that the sole exception to the above, that I am aware of, other than cryptographic devices, resulted from ARPA-supported research in the MULTICS project at MIT. ARPA has been a major source of support for research on computer security.

As you will soon see, I am greatly concerned with the application of information processing technology to surveillance. That being so, why have I defended networks? The answer is simple—I think they have been getting a bad reputation.

INTERCONNECTION OF GOVERNMENT COMPUTERS

I understand there is some sentiment for legislation forbidding the inter-connection of any government computers. I personally think that's throwing the baby out with the bathwater. If there is concern about the FBI computer being programmed to penetrate the Social Security computers, and the Census Bureau computers, then treat the files of Social Security and the Census like classified information. That is, don't let them be accessible from the outside until the technology exists to satisfy those concerns necessary to safeguarding classified information. But don't generalize to all government computers.

Note that the FBI computer is already on a network. While I suspect that as much security was built into that system as could be rea-

sonably purchased at the time, the chief source of leaks from those files is that tens of thousands of law enforcement personnel have a legitimate reason for access to the files. While the wholesale transfer of information may be difficult, individual files can be copied rather easily.

RECOGNITION OF SPOKEN WORDS

Let me briefly mention another area of research in information processing which, though being carried out for quite other reasons, is also related to surveillance. I refer to speech understanding, sometimes referred to as voice recognition. By this I don't mean the identification of the speaker as in voice prints, but rather the recognition by a computer of what words have been spoken, so they can be entered and stored in the computer just as though the words had been typed on a terminal connected to the computer.

One reason for wanting this capability is so that we can input information into a computer orally. The goals of research in this area today are not terribly ambitious, yet even so, they are elusive. The hope is to get the computer to be able to understand a few dozen words, spoken by a small number of cooperative people whose voice characteristics the computer knows in advance.

LISTENING TO TAPES RESULTING FROM SURVEILLANCE

This technology is related to surveillance because a bug, or a tap, results in miles of tape recordings, most of which is of no interest to the goals of the surveillance. Transcribing all that tape is expensive—just listening to it is expensive.

I do not mean by the above to suggest I believe that research in speech understanding should be stopped because it might be used in surveillance, though I am aware of computer scientists who have refused to work on such projects for exactly that reason. But, as speech understanding capability increases, we must recognize that surveillance capability does, too.

Before leaving this topic I should also observe that the surveillance situation is usually more difficult than recognizing a few words for computer input, because here the speakers are not trying to cooperate and their voice characteristics may not be known in advance.

ELECTRONIC FUNDS TRANSFER SYSTEMS

Let me now turn to a new topic. Several times I have referred to situations where the technology under discussion was developed for reasons other than surveillance, but it happens that it is useful for surveillance purposes. As a prime example of this I want to talk about electronic funds transfer systems. I can't give you a detailed definition of an electronic funds transfer system (usually referred to as EFTS) because the system hasn't been built. Its final form will be an outcome of intensive competition, and also of government regulation. But the general form is reasonably clear. Terminals will exist in stores, hotels, restaurants, etc. (where they are referred to as point-of-sale terminals), and in financial institutions, including unattended terminals miles from the nearest office of the institution. In short, terminals will

be at any location apt to have a large number of non-trivial financial transactions.

Let's look at one way it might work. Say you are about to buy a book. You present your card (sometimes called a "debit card", although National Bank-Americard calls theirs an "asset card") to a clerk who puts it into a terminal which reads it and then calls up your bank. If you have enough money in your account, or if your bank is willing to grant you that much credit, the transaction is okayed; your account is debited; and a credit is dispatched from your bank to the book store's bank account.

THREE FACTORS THAT YIELD SURVEILLANCE GOLD

The dimensions of the final form of EFTS which are of importance to its potential surveillance capability are such things as the percentage of the transactions recorded; the degree of centralization of the data; and the speed of information flow in the system.

Suppose for a minute all transactions over $10 must go through the system and that they are immediately debited to your account in your bank's computer. Thus the system not only collects and files a great deal of data about your financial transactions—and that means a great deal of data about your life—but the system knows where you are every time you make such a transaction.

Suppose that the rule for all transactions over $10 is not compulsory, but voluntary. And further suppose that you have gotten into the habit of using the system because: one, it is convenient; and two, it may be cheaper than other payment mechanisms. Now comes an instance in which you want privacy and decide to use cash. If you have to obtain the cash from the EFT system, that cash transaction will stand out like a sore thumb. The point here is that it's not enough just to have the option of using cash, the cash option must be used frequently or it becomes useless as a means for privacy.

To give you an idea of how powerful a surveilliance system an EFTS would be, consider the following. In 1971 a group of experts in computers, communication, and surveillance was assembled and given the following task: Suppose you are advisors to the head of the KGB, the Soviet Secret Police. Further, suppose that you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. Further, the system is not to be too obtrusive or obvious. Not only would it handle all the financial accounting and provide the statistics crucial to a centrally planned economy; it was the best surveillance system we could imagine within the constraint that it not be obtrusive.

That exercise was almost four years ago, and it was only a two-day effort. I am sure we could add some bells and whistles to increase its effectiveness somewhat. But the fact remains that this group decided that if you wanted to build an unobtrusive system for surveillance, you couldn't do much better than an EFTS.[5]

PREVENTION OF ABUSE OF EFTS

Naturally, the EFTS proponents believe that laws could be written to prevent abuse of the system. I am less sanguine. I'm not concerned

[5] The Center for Strategic and International Studies, Georgetown University, October 29–31, 1971.

about the bankers invading my privacy or using the system for surveillance purposes; but I am afraid that EFTS system operators may be unable to resist pressures from government to let the EFTS be used for surveillance.

There are in existence today computer systems which could be used in exactly this way, although the number of financial transactions involved is comparatively small. What I have in mind here are the credit authorization systems of National Bank-Americard, Master Charge, American Express, and various check authorization systems. All can have individual accounts flagged. If an individual tries to make a purchase, or tries to cash a check, the system is interrogated. If the account has a special flag the police (or whoever) can be notified where that individual is at that very instant. Check authorization systems are especially subject to such abuse because they depend on the police for information about bad check passers and for information on forgers for their computer data bases. I have no doubt that such systems have already been so abused.

WHY BE CONCERNED?

Why should we be so concerned about surveillance? I don't think I can put it any better than Henry Goldberg did in a recent speech:

> 1984 is really a state of mind. If you are always tied to the consequences of your past activity, you will probably adopt a "don't stick your neck out" attitude. This would create a pressure toward conformity, which would, in turn, lead to a society in which creativity would be an early victim and the democratic ideal of a citizenry with control over its own destiny would not flourish for long.[6]

In a recent speech Professor Philip B. Kurland pointed out that we will not celebrate the 200th anniversary of the U.S. Constitution until 1987, and that before we can do so, we must successfully get past 1984. He further said that if he were in charge of some Bicentennial celebration, he would require all participants to read Orwell's "1984" to show what the new nation was created to avoid.[7] I would extend the advice to those concerned about electronic funds transfer systems. And to "1984" I would add the recently published "The War Against the Jews—1933 to 1945",[8] and Tom Houston's memo on domestic intelligence, which was issued to all American intelligence agencies in President Nixon's name on July 23, 1970. The book "1984" shows what might happen; the latter two documents detail actual events.

[From Communications of the ACM, September 1974]

A Report of the ACM Committee on Computers and Public Policy

The ACM Committee on Computers and Public Policy comprises Daniel D. McCracken (chairman and drafter of the report), Paul Armer (vice chairman), Robert L. Ashenhurst, Herbert S. Bright, Jerome A. Feldman, Roy N. Freed, John King, Rob Kling, Peter G.

---

[6] H. Goldberg, "Impact of the Less Cash, Less Check Society," presented at a meeting of the Computer and Business Equipment Manufacturers Association, May 28, 1975.

[7] P. H. Kurland, "The Unlearned Lesson of Watergate," Wall Street Journal, June 17, 1975.

[8] L. S. Dawidowicz, "The War Against the Jews—1933–1945," Holt, Rinehart, and Winston, New York, 1975.

Lykos, Susan Nycum, Lee L. Selwyn, Bruce W. Van Atta, and Joseph Weizenbaum.

The Committee on Computers and Public Policy of the Association for Computing Machinery is concerned by its charter with the broad area of the interaction between computers and people, focusing on the interests typical of legislative and regulatory bodies. Its functions are: to advise the ACM Council, as appropriate; to serve the educational needs of ACM members and the general public in this area; and, if requested, to provide consultation on the technical implications of proposed legislation. The committee is not authorized to speak on behalf of the Association, and is prohibited (as is the ACM itself) from any activity that could be construed as lobbying. The committee may attempt to state and clarify issues, as in what follows, but it may not state ACM policy on any issue.

The committee foresees the need to revise this report periodically as problems change or are resolved and as new ones arise. Accordingly, comments and suggestions are solicited, either on questions of substance or on ways of improving the presentation to better achieve the purposes of the paper. Such comments might suggest areas on which the committee could concentrate its further efforts, and might also be useful to the Council in its work.

A PROBLEM-LIST OF ISSUES CONCERNING COMPUTERS AND PUBLIC POLICY

This paper is a listing of some of the present and potential problems which arise at the intersection of computing and public policy in its various aspects. There is no attempt to break new ground, which would be difficult when, already, the topics covered are the subjects of a small library of books. The intention, rather, is to serve the needs of people in both parts of the intersection. It is hoped, for instance, that this report will be useful to lawyers and law students who desire guidance in this rather new area. It is hoped, likewise, that it will be useful to computer scientists and computer science students, e.g. in seminars on the social implications of computing. As another example, it might be useful background reading for staff members in Congressional offices.

In other words, the paper is intended to be a summary of some of the issues that impinge upon both computer science and the general public (and its representatives). It will not tell a lawyer anything about the law that he does not already know, but it might give him some new insights into the legal implications of computer technology. It will not tell the computer scientist anything new about computer science, but it might expand his understanding of the social aspects of his work.

The term "public policy" is intended to be taken not only in the usual sense of denoting the concerns of legislative and regulatory bodies, but also in the broader sense of what is good or bad for the social fabric as a whole whether expressed in the form of laws or not.

The document is not intended to be in any way polemic. If some of the questions seem to contain implied answers, or if any of the presentations are onesided, it is not intentional. In most cases the questions that follow the statement of an issue present various contradictory

viewpoints, which fact is simply indicative of the present state of discussion of the issues.

And, to repeat, the paper does not in any way represent a statement of position on any of the issues by the Association for Computing Machinery.

1. Information Services for Home Use

Background.—The advent of widespread two-way cable communications, such as for television, has opened up numerous opportunities for information process services. The channel width is adequate for carrying a great many data and/or voice channels in addition to regular TV programming. Some have predicted that this development will completely revolutionize everything from libraries to politics; others have looked at economic and other factors and predicted a much more limited use.

Questions

1. Here is a list of some of the uses that have been suggested which ones are really likely to come to pass? Vote casting, the instant national referendum, home-study courses, other instructional uses, advertising, news, stock quotes, weather, bank transaction accounting, shopping for groceries or department store items in conjunction with "electronic money" concepts, reference lookups replacing some uses of libraries, private-mail service, alarm monitoring, automatic reading of utility meters, calculation services, poison control center services, personal data storage and retrieval, checkbook reconciliation, game playing and instruction for the bed ridden, and municipal services information. The list can readily be extended.

2. Should an information utility be public, private, or private but regulated? The not entirely happy history of telephone and television suggests that none of the three is perfect.

3. If some such developments are essentially inevitable (we do not mean to suggest that they are), would it be wise to hasten a merger of the fields of computers and communications so that we will not later be burdened for decades with "black boxes" needed to marry the two? If so, who should be in charge? So far the major telephone company and the major computer company have been deterred from encroaching on each other's fields by antitrust action or the fear of it. Without arguing whether that has been beneficial up to now, is it the best way for the future?

4. Cost aside for the moment, are all of these good ideas from a broad public policy viewpoint? Would they tend in the direction of creating an even greater isolation of people from each other? Is the trip to the library or store a good thing in secondary ways? Are there desirable features in attending an adult education course in the company of other people, rather than learning the same material via TV all by oneself? In other words, is there a danger that we are so fragmented that a trend toward further fragmentation is undesirable?

5. In view of some of the trends in the use of computers, it has been suggested that soon the only persons who will "exist," in practical economic and political terms, will be those whose identifications are accessible through computers. All others will be totally powerless except within a possible underworld populated by others like them.

Is this an exaggeration? If true, is it bad? Do the benefits justify requiring a person to have a computer-accessible identification in order to participate in the functions of society? Or are these threats to society as a whole, or to some individuals, sufficient to make us hesitate before we pursue such a future with abandon?

6. What, in fact, are the economics of specific proposals? It is common for people to run through a list of ten things that are technically possible, then indulge in some armwaving to the effect that, with so many possibilities, the economics will work out *somehow*. Is this true? Is there any chance that the economics are extremely unfavorable and that people might not really be interested in any one of the possibilities at the level of a monthly cost roughly equivalent to that of a payment on an automobile? In other words, how much chance is there that the whole thing is only a fad that will die out when faced with the harsh economic facts?

7. How much impact would an information utility have on our mobility habits? By way of analogy, the automobile made the suburbs possible, with walking for any purpose other than exercising the dog becoming regarded as strange behavior. (A man in Los Angeles was once stopped by the police because he was walking down a street in a residential neighborhood. Very strange!) If the idea of an information utility were to catch on in a big way, it would significantly reduce the number of occasions for people to leave their homes. Already shopping centers are being built around automotive needs as the center, with such things as grocery stores being essentially satellites of the gas station. Could something like that, translated to computer terms, happen with the information utility? What form might it take? How would the good and bad aspects balance? For example, would supermarkets begin to disappear, to be replaced by telephone shopping to a computerized warehouse? Serious and wide-range thinking about these effects is very much in order right now. What will our daily lives be like a generation from now if all the things that some enthusiasts have predicted for the information utility should actually occur?

8. Can security and privacy be protected effectively in such a system? Systems which are much less extensive and ones with elaborate security provisions have been broken by clever college students.

9. Could and should the owner/operator of the information utility be enabled to use the information flowing through his system, such as analyzing buying patterns for the benefit of stores, or for selling as mailing lists?

10. It has been proposed that the marriage of computers and communications makes possible what has been called the instant national referendum, in which people would be presented with a question of importance via TV, to which they would respond by pushing appropriate buttons that would enter their answers into a computer for tabulation. There doesn't seem to be too much doubt that it could be done: the question is whether it is desirable. Could the issues be presented adequately in this way? Would such ease of voting over-represent the casual opinions of people who didn't really understand the issues?

79-064 O - 76 - 35

One of the advantages of the relatively clumsy procedural requirements of legislatures is that they reduce the incidence of bad laws which might be passed in response to momentary issues of passion. Would the legislative process as we know it survive the use of computers and communications facilities to produce fast response on current issues?

11. A service of the type under discussion might not be terribly expensive, but it could hardly be really cheap either. Would this not spread the gap between the haves and the have-nots? Should public policy dictate some form of subsidy so that the new service could be available on some minimum basis to everyone? Would minority groups suffer loss of power?

12. How much danger is there that the whole system, which would naturally be a vast undertaking, would come to be looked upon as Big Brother? How much effort would there be to sabotage the system, and how well could it be protected against sabotage?

13. Might a good information utility bring back the "town meeting" in a new form, to be sure, but with direct citizen participation in local government? Would such a system permit filibustering? Would it speed up or slow down the pace of government?

14. How much danger is there that the contents of the data banks available to the public would come to be, in effect, a definition of the truth on those subjects? It is instructive to recall that the Department of Defense was able to mislead the entire United States public and almost everyone in the United States government about the bombing in Cambodia simply by producing computer printouts falsely describing the targets that had been hit. Naturally, the power to control information flow is always subject to abuse and must sometimes be held answerable to public regulation computers or no. But new technology often reveals new facets of old problems. Is this such a case?

2. Computers and Money

Background.—Rapid changes are taking place in banking and related fields, such as credit cards and department store record keeping. Credit card transactions, even for relatively small amounts in some cases, are routinely checked against computer based files before the credit is granted. Banks increasingly have on line teller terminals and unattended banking facilities. Point of sale recorders for retail establishments are currently an exploding market.

Questions

1. Is a new definition of money needed? The checkless and/or cashless society will not take over 100 percent of money transactions soon, it ever, but something in the range of 50 percent is easy to imagine within a decade or so. Under such conditions, whole new sections of law would have to be rewritten. (The current Uniform Commercial Code, which governs most such matters, does not contain the word "computer.")

2. Is the trend toward stock "certicates" that exist only in computer form a good thing? Are new laws needed to control this?

3. Are these really policy questions, or is it more a matter of public acceptance of computerized records? What *is* the present public attitude?

4. What are the privacy implications of the Electronic Funds Transfer System being urged by the Federal Reserve Board? With all information that is now written on a check being in electronic form, it would be a simple matter to collect information on, say, the contributors to political groups considered to be nonconformist. If this information is acquired through a federal agency armed with a subpoena, it might be perfectly legal—but is it desirable? Would fear of such surveillance strongly inhibit many people from supporting nonconventional groups? If such a system were tied in with point-of-sale recorders in stores, it would be a simple matter to tell where a person is at the time of any transaction, and thus, also, develop a record of an individual's travels over a period of time. This is much more difficult (and therefore less likely to be done) under present methods. Are the banking and economic factors strong enough to outweigh such considerations? In other words, is the system really needed, as seen by the individual consumer/citizen?

3. Computers and Elections

Background.—Computers have an impact on several aspects of the voting process. As everyone knows, they are used to predict the outcome of elections on the basis of early and fragmentary returns from districts that have proved in past elections to be good predictors. A computer is used to tally votes in the House of Representatives. Computers play a role in opinion surveys that often seem to be self-fulfilling prophecies. And a modern campaign for a major elective office cannot be run without a computer to generate mailing lists and otherwise keep records. There has been much talk of a national individual voting system through terminals in the home, presumably connected through TV facilities.

Questions

1. Is it good or bad that members of the House of Representatives must be physically present on the floor in order for their identification cards to be placed in the voting machine? It would obviously be possible to place vote-recording devices in each Representative's office, but would the presumed benefit of faster voting and less time wasted walking through corridors more than offset the drawbacks of uniformed voting, for instance, that might result?

2. The Presidential elections can be "called" by the sophisticated prediction programs that analyze returns from just a few key districts. The prediction of the outcome, in fact, can often be made long before the polls close in the western states. The effect is indirectly to disenfranchise the western voters, since they can see no point in voting in an election that has already been won. But what if the election was really close, so that all the people in California and Hawaii who decided not to bother going out to vote might have swung it the other way? Is that democracy? Or how about the local elections that are slighted because the voters no longer have a Presidential race to draw them out to the polls? Should ACM go on record as urging that no national predictions be made until all polls are closed everywhere in the nation?

It has been pointed out that to enforce such a ban could be interpreted as a violation of the First Amendment rights of the press; is this a valid objection? If it is granted that there is a problem here, are there better solutions than a ban on predictions?

3. A computer is a very powerful tool, and as Francis Bacon said, knowledge is power. If one side has access to a data bank of potential contributors, simply because it has more money, is democracy being well served? Does the use of the computer make it easier or harder for a candidate to say one thing in one district and something else in a district with different ethnic and economic characteristics? Should there be some equivalent of the equal time law, whereby each candidate is somehow guaranteed some minimum amount of computer power?

4. Are there ways that computers might assist in the legislative process, at any level, other than by computerized voting? One thinks of the imbalance at the federal level between legislative and executive access to computers for research, information retrieval, and computer modeling, for instance.

5. Most national elections are participated in by only 50 to 60 percent of the eligible voters. Could computerized voting raise this to 90 percent? Could the registration process, residency requirements, and other procedures that are designed to prevent a person from voting more than once all be eliminated by a single vote to a computer? Would such changes have any impact on the efforts of those who would like to reform the Electoral College?

4. Computers and Education

Background.—At one period in the nineteen sixties it was widely believed that the use of computers would revolutionize education. Students were pictured sitting at typewriters connected to computers, the computer interacting with the students to provide at least as good instruction in some areas as a human teacher, at less cost. Such systems have turned out to be much more expensive than expected, and it has developed that writing the computer programs required is a very difficult task and that there are not very many people who can do it well. There have been some successful experiments, but the idea has not gone far enough to establish whether or not it would be educationally sound and economically feasible if carried out on a large scale.

Questions

1. Is the promise still great enough that the effort should be continued, with attempts to get adequate support from governments and foundations?

2. If any such system did catch on, how would the function of the teacher change? Most investigators in this area see no reduction of staff, but if teachers are dragging their feet, is it because of fear of unemployment or because of resistance to change?

3. Might disperson of the educational process be one outcome of a success in this area where students spend more time at home and less in school? If so, would that be good or bad public policy?

4. There is some question whether hand-held calculators are to be defined as computers, but there is no doubt that they will have a concrete impact on education at the college and high school level. (Instructors already have to rule on whether calculators are permitted on exams.) Is this trend to be deplored or encouraged? Are calculators simply supplementing not-too-important arithmetic skills, leaving the students free to concentrate on more important ideas? Will their use

lead to a nation of people who can't add or multiply without mechanical assistance, and if so, is that good or bad?

5. The Computer as a Metaphor for Human Self-Understanding

Background.—Joseph Weizenbaum, in an article in *Science*, May 12, 1972, developed the idea that computers give us a new way of thinking about ourselves, much as the microscope changed the view of disease or as the synthesis of urea in the 19th century proved there is no essential chemical difference between organic and inorganic processes. The first example weakened the notion that disease is a punishment for sin, and the second struck a major blow for evolution both have greatly altered the way people look at themselves.

Weizenbaum, drawing on the work of Berger, Luckman, Mannheim, and others, in what is called the sociology of knowledge, suggested that the computer may provide us with a new way of seeing ourselves that will be of greater impact than anything that has ever happened before. Here again the strange paradox of compartmentalized thinking shows itself: people think less highly of themselves as they see computers playing passable chess or predicting the weather, yet they are willing to believe almost any excuse that involves some such statement as, "It was a computer error."

Weizenbaum also discussed the phenomenon of the inevitability of technological growth described by Jacques Ellul in *The Technological Society.* People ask, Will it work? when they ought first to be asking, Should it be done at all?

Questions

1. If the notion of computer as one metaphor for human self-understanding is correct, this factor would easily be more important in the long run than anything else discussed here. But is it a primary effect, or is it a lesser side effect? Is it a public policy question? Is there anything a lawyer or a legislator could do about it? Might ACM try to provide a document on the issue for the use of writers (editorial writers, novelists, essayists, etc.), and then attempt to get it widely distributed? Or is the best procedure simply to do our job right so that there will be as few *false* "facts" as possible for writers to draw upon?

2. Is the point true? Is the analogy between the microscope and the computer valid? Are there factors working against a sense of identity between people and computers?

3. One of the central features of the theory of the sociology of knowledge is that institutions, which are after all human creations, come to be objectified and then impact people as though they had an objective existence independent of their creators. For example, government is only people—what else could it be? But that isn't how it *feels* at income tax time. Is there a computer analogy? Does the often-heard phrase "the computers says" signal the beginning of an era when computers will be the most independent of all human creations? Is that good or bad? If bad, can it be stopped?

4. Might computers some day "outthink" human beings, perhaps by formulating a natural law that fits the facts but which cannot be proven or disproven by human thought processes? If this were to happen, what would be the impact on human self-understanding?

5. One of the side effects of the requirements of computer programming has been an enforced logical review of processes in organizations, since programs so far can usually deal only with ordered and quantified processes. This is a proliferating side effect. Is it widely recognized? It is good or bad, on balance? Does it lead to an identification of the real with the quantifiable? Should it be exploited or guarded against?

6. Is society dependent upon repetitive processes for its own sanity? If all "mundane" acts, such as washing cars, threading nuts on bolts, etc., were left to the control of computerized systems and only creative tasks were left to human beings, could society survive? More concisely, the question is: Can we sustain continuous creative thought, or must it be interspersed with routine tasks—tasks that are rapidly being automated?

7. There is a concept of the "tyranny of small decisions" that seems to indicate that a number of small, relatively trivial decisions early in a process reduce the options and alternatives available later at a policy level. Bureaucratic structures exhibit this process. If computer systems come to handle a larger and larger share of small decisions, would they, in this fashion, constrain policy options in a way that would impact on human selfunderstanding?

6. Computers and Privacy

Background. One of the most widely discussed issues relating to computers is that of data banks and the individual's right to privacy. As this is written, half a dozen bills on the subject are before Congress, TV documentaries are being devoted to it, and articles appear weekly in both trade journals and the general press.

As with most questions of public policy, the problem is not whether a particular right is legitimate but that it comes into conflict with other rights. Although the absence of precise definitions poses a difficulty in itself, most people would agree than an individual has some right to keep information about himself from inspection by the general public, assuming the purpose of doing so is not in the service of criminal acts. The conflicting right is that of society as a whole to have certain kinds of information that contribute to the general good. For example, most people would agree that a person should not have information about criminal acts in his distant past held against him forever yet statistical (non-individualized) information about crime trends is usually thought to be valuable. Since maintaining the data needed to provide statistical trends holds the possibility of abuse of data about individuals, the two rights are in conflict. Finding a proper balance between these goals is one of the most difficult aspects of this issue, and yet it must be attempted.

Questions

1. Some of the questions that have most commonly arisen in the discussions of data banks include the following. What right should the individual have to ascertain whether the information about him is correct and to force correction of errors? What penalties, if any, should be imposed on administrators of data banks for disseminating false information about an individual? What right does the individual have to know what collections of data about him are in existence?

What kind of time limit should be placed on the holding of damaging information about an individual, such as his past criminal record? Who has a legitimate right of access to information about an individual? Does an individual have a right to know who is given access to data about him? What safeguards need to be placed on the interchange of information by various agencies holding data about an individual? Should this interchange be deliberately curtailed by prohibiting the use of a universal identifier such as the Social Security number? Does Congress have a clear Constitutional right to regulate the interchange of data between state agencies? (In what way does data fall under the Interstate Commerce clause, for example?) Does Congress have the power to regulate the use of personal information by individuals? By corporations? What are the First Amendment limits?

2. Do we have an adequate definition of "privacy"? I have no objection if my bank branch manager looks at a computer printout for information about me before approving my loan, but I object strenuously if he shows that printout to anyone else, including bank employees who have no "need to know." And I object if a large number of government agencies claim a "need to know" when I am unable to understand the basis of the "need." On the other hand, the right is surely not absolute; if someone wants to record my habits in walking my dog on a public street, I may be annoyed, but I can't really stop him so long as he doesn't actually harrass me. Where does one draw the line? Exactly what *is* the "right" to privacy?

3. Some kinds of statistical surveys seem so obviously beneficial for the greater good that a small loss of privacy is clearly negligible. The Public Health Service needs to know about an epidemic as soon as the possibility shows up. But what if the epidemic in question is VD; does society have a right to force people to disclose sexual partners? And even then, are permanent data banks necessary?

4. The conflict between privacy and legitimate public knowledge has existed for ages, going back at least to the Hebrew prophets who shouted from the housetops secrets that kings would have preferred to keep to themselves. Has the advance of the computer changed this situation materially, or is this, too, just a case of providing a better tool for something that has been going on for ages? If it is the latter, are there any really significant public policy issues? Recent studies have certainly suggested that there is a problem, but in those studies was the right of society to know given a fair defense in its opposition to the right of privacy? Or, granted that both goals are good, does the coming of the computer nevertheless demand new rules and a better understanding for working out satisfactory compromises?

5. Implicit in many discussions of data banks and privacy is an assumption that the information in question does need to exist—that the only *issues* are things like accuracy, longevity, and rights of access. But should it not be asked in each case whether the data needs to be gathered in the first instance? Should not the very existence of the collection of information have to be defended in terms of the benefits to society?

7. Computers and Employment

Background.—The impact of computers on employment has been a major concern of many people, especially labor leaders, since the

earliest days of the computer era. Although computer work has created hundreds of thousands of new jobs, it has eliminated or modified a great many others. Even if computing has created more jobs than it has eliminated—and the statistics do not make this completely clear—some of the individuals displaced have found it difficult or impossible to retrain for new work.

Questions

1. The introduction of new technology always creates some displacement of workers, as old skills become less important and new ones become necessary. Are there differences in this case that require explicit public policy responses?

2. What in fact has been the net impact of computers on employment? Why are the statistics so hard to assemble? Is it a question of definitions? Are there too many cases where a diversity of factors is at work, making it hard to separate causes? How serious is the ambiguity caused by lumping "computers" with "automation," recognizing that, although most automation does involve computers, the two are not identical.

3. What does the pace of technological change in computing do to the job security and the retraining needs of workers within computing? How rapidly does a skilled and capable computer person become obsolete if he does not constantly engage in continuing professional education?

4. How much impact has the introduction of computers had on job conditions and job satisfactions? Do a great many workers feel that they are merely cogs in a machine? Do many feel that the opportunity to exercise individual initiative and creativity has been decreased to the point of overwhelming boredom in their work?

8. Computer Literacy

Background.—The general public seems to hold two diametrically opposed views. (The ability to compartmentalize one's thinking in this way is well known from psychological studies.) On the one hand, most people will accept at face value statements that their credit card bill, their bank statement, their airline reservation—whatever got fouled up "because of the computer." (Whether it is true occasionally is not the point here.) On the other hand, most people will quickly believe the most outrageous ideas if it is emphasized that the work was done with a computer. No matter that the results are false or trivially obvious; no matter that the same false or trivially obvious results could have been obtained with pencil and paper—the computer said it, and the computer never lies. The notion that a computer can only follow an algorithm that defines the procedure in total detail and that a computer can do nothing that a person, given enough time, could not do, simply has not penetrated the public consciousness. As a result, some very strange assertions have come to be common "knowledge." (For one random example, many people seem to believe that it would be simple to get a computer to beat Bobby Fischer at chess: "You just have to program it.")

Questions

1. Who is at fault here? Did we do too good a job in the fifties and sixties with "gee whiz" speeches? Is the public so gullible that it will

believe anything whatever as long as it is intoned by a man in a white lab coat who has computer printouts in his hand? Is it somehow in somebody's interest to perpetuate this kind of misconception?

2. Who could best do something about it? Should we in the profession go to work, speaking at schools and Rotary Club meetings, and meetings of other professional societies? Should we be encouraging the writing of good solid books for the layman? Should we send a delegation to visit the major publishers of secondary school books? Should there be a drive to make a "computer appreciation course" required for every college graduate? Could such a course be developed, so that, taught by thousands of instructors (some of whom are not themselves very well informed), it would still accomplish the purposes? Exactly what should be in a text for such a course? Is some direct computer experience an essential part of such a course, as many believe?

3. What can be done in the short term to help enlighten key people in important decision-making positions? As one example, judges who without specific background in the subjects, have to rule in antitrust cases involving computer companies, decide the admissibility of computer printouts as evidence, evaluate computer software for taxation purposes, and the like.

4. One manifestation of the problem of computer literacy is the willingness of some people to accept fantastic claims for such things as computer-manufactured horoscopes and computer dating. We recognize that many people believe in astrology and that computer dating sometimes works out just fine, but we deplore the use of computers to defraud people who become convinced that computers can do things for them that if not impossible are, in any case, worth much less than is being charged.

What should the role of the professional organizations be in such abuses? What is the proper role of government? (Some states are already acting, either through the passage of laws or through intervention by their Attorneys General.) Can the problem be effectively attacked by attempting to educate the public directly? On the other side of the coin, is there a question here of the First Amendment rights of companies engaging in such activities? That is, is there a sense in which the exercise of computer power is an exercise of free speech?

9. Computer Science and Data Processing Education

Background.—From a point a mere 20 years ago when there were no formal courses in the design or use of computers, we now have dozens of schools offering Ph.D. programs, hundreds offering full programs if not actual degrees at the bachelor's level, and many hundreds of schools at the two-year level offering training in programming or computer operations, plus some hundreds of commercial concerns offering training in programming or computer operations.

Questions

1. Are we training the right number of the right kind of people? Are there too many or too few Ph.D.s in computer science? Are they trained in areas where they are most needed? Is the average computer science graduate too heavily oriented toward theory that will be out of date in a few years? Is his training too theoretical, or is a highly

theoretical training the only way to avoid the rapid obsolescene that would follow upon a too-practical sort of education?

2. How much responsibility do the schools have to lead the way in theoretical advances such as better languages, compilers, sorting methods, etc? Are the schools closely enough attuned to the real needs of the field to judge wisely what to concentrate research upon?

3. Are the schools at the two-year level, as well as the commercial data processing schools, turning out students who are employable? Are they attracting minimally-qualified students with the lure of high pay, only to produce graduates who cannot really perform? If so, is that altogether bad? (Such students may still be benefitted in other work they turn to.)

4. How much governmental regulation of data processing schools is desirable, and what kind? Should there be restrictions on the kind of advertising permitted? Should there be enforced standards on who can enter, to prevent the schools from taking money from people who are grossly underqualified? Should course content and amount of computer time be regulated? How does one balance the need to regulate unscrupulous operators of the worst schools against the legitimate right of freedom to carry on a business? Should the professional associations take a position on certification of schools?

5. Various groups from time to time propose curricula for various types of training. These are beneficial when used intelligently, and harmful when followed slavishly.They have a very strong influence on book publishers. Without suggesting that there have been serious flaws in the past, is there any way the job can be done better?

6. Should professional organizations in the computer field become involved in the accreditation of academic programs and departments, as is done in some other technical fields?

10. Liability Questions

Background.—The computer is at the heart of many businesses. A few businesses have already gone bankrupt because of irremediable computer foul-ups, and if rumors are to be believed, a lot more have come close. Since a computer does so much in a short time, and since so much data is concentrated in one place, the computing function becomes crucial, and the people in it have a great responsibility as well as a great opportunity for mischief, malicious or not.

Questions

1. Who is responsible when computer programs fail? The system designer who may not have adequately defined the job? The programmer who made a mistake which he failed to catch because of inadequate program testing? The manager who did not allow enough time for proper testing? The computer operator who, although it was not his prime responsibility, did notice what he thought might be a problem—but said nothing? Regardless how these questions are resolved, are there public policy issues here? By analogy, a worker who shuts down an automobile line for a couple of hours because of some kind of carelessness may be reprimanded and/or fired, but he does not come into legal problems unless the act was deliberate and malicious. If a system designer or programmer makes a big blunder, how can anyone determine objectively whether or not it was deliberate?

2. Who should be held responsible if a poorly-secured time-sharing system is "burglarized" by an employee of a rival time-sharing con-

cern who had made proper arrangements to be a paying customer? Is it a public policy question that some users occasionally find ways to defeat the accounting system so as to get free time from a time-shared computer? If a time-sharing customer finds a way to defeat data protection features and gains access to data other than his own, has he broken any law? If no present law covers such a situation and a new law were to be drawn, whose interests are primary—the management of the time-sharing concern or the customer whose data was copied? Is the law supposed to try to determine what the intentions of parties were, if those intentions were not spelled out contractually?

3. Should those who provide computing services be held responsible to consumers? Should the store that ignores your notification of an error in your bill, caused by programming error, be penalized? Where does liability lie if a lawnmower produced by a computer-controlled factory explodes? Could a firm ever be held liable because it did *not* use a computer when such use would have prevented injury to a consumer?

4. The Uniform Commercial Code imposes an implied warranty of fitness of goods. Is this applicable to computer programs, or should it be?

5. Would the licensing of programmers and other computing personnel be a useful approach to some of these problems?

11. Monopoly Considerations

Background.—Questions of the size of computer firms have been a part of the field since its origins, a government suit against Remington Rand and IBM having been filed in 1932. Domination of major product areas by three or four firms is true of most American industry; why the computer field should have been dominated by one firm is unclear.

Questions

1. Is there something about the computing field that inherently pushes it toward bigness? Is the investment for entrance required so high that only firms with huge capital resources can succeed? The experience of RCA and General Electric would seem to argue in that direction, but the success of Control Data Corporation and Digital Equipment Corporation argues the opposite.

2. How bad is bigness? There are clear advantages in terms of support of research and development, and clear social disadvantages in terms of withholding new developments until investments on earlier projects have been recovered. Thinking only of technical and financial factors as seen by the customer and therefore by society, is bigness good or bad, on balance?

3. If a computer company is to be "broken up," on what basis should it be done? If done along hardware size lines, rapid changes within the field may turn the newly organized group of companies into merely a different form of monopoly. If done on the basis of the split between hardware and software, the effect would be to create a new monopoly in the software area, since hardware will continue to become less and less important in relation to software.

4. How should the data processing field be defined? (The impact on antitrust enforcement is significant.) Does IBM supply computers or problem-solving power? Do disk storage devices contstiute a sepa-

rate market from computers in general? If antitrust legislation is to be applied to a variety of submarkets, what are they and how—from a public policy standpoint—should they be defined? (For example, if disks and tapes are considered to be separate markets of the same size, then a firm that sells 80 percent of all disks but no tapes would have most of the disk market and perhaps be monopolizing it, but if disks and tapes are considered together, the firm would be selling only 40 percent of the total.)

5. If we face an extended period of litigation on this issue, how should the costs be allocated? Defending an antitrust suit can cost tens of millions of dollars: is it in the public interest that a company should have to bear all this cost? On the other hand, is the Justice Department adequately staffed and budgeted for the task?

12. Computers and Patents/Copyrights Trade Secrets

Background.—Much work is being done on the question of protection of the rights to intellectual property. Patent and copyright laws are both overdue for the major changes that will be enacted in the next few years, quite apart from the special problem of the protection of programs and data. On these latter topics it has to be said that there is confusion about what a patent or a copyright protects, and about how the content of the intellectual inventions is to be expressed.

Questions

1. Not everyone agrees that computer programs (software) should be protected, by any method. What are the countervailing arguments? Would extensive patenting of programs inhibit growth? Could licensing fees be held low enough that the root meaning of patent ("open") could come into play?

2. Generally speaking, the real content of what a developer would want to patent or copyright is the algorithm that expresses it. (An algorithm is a precisely defined sequence of processing operations that leads to the solution of a problem.) An algorithm can be expressed in English, in the graphical form of a flowchart, or in any of the dozens of computer languages—and still be the same algorithm. How can a judge and a jury be expected to understand this and thus make an intelligent decision, faced with, say a Fortran program, a flowchart, and an English description—all representing the same algorithm? In short, how *should* algorithms be represented so as to bring about the most fair administration of justice? Would it be useful to experiment with "technological courts," or with special masters appointed by a judge to take specialized evidence?

3. The concept of data and ideas as intellectual property is well established in law. Stealing a trade secret by photocopying a blueprint, for instance, is clearly illegal, and it is no defense to say that nothing was stolen since the owner still has use of the original. In at least one case, in California, a court held that theft of a program from a computer by telephone was a criminal violation of the trade secret laws.

Yet there seems to be some uncertainty how these concepts apply to new technology. It is perhaps not yet fully understood that data is an abstract concept having almost nothing to do with the form of

its representation. Whether a firm's confidential data exists as marks on paper, holes in cards, magnetized spots on disk or tape, charges on capacitors—or in somebody's head—is largely immaterial. This and related notions will come to be well understood in time; is there anything that might be done to speed the process?

4. Have we in the computing profession done our part of the job by providing clear and concise definitions of important terms such as data, program, and algorithm?

13. Computers and Electronic Transmission

Background.—The demand for good facilities to connect terminals to computers and computers to each other is now becoming acute, as the volume increases exponentially. It has been estimated that 5 to 10 percent of all telephone use is now for data, and that the figure will be closer to 50 percent within the decade.

Questions

1. Are present rate structures appropriate for a world where half of all telephone use will be for data communications? Should rate structures encourage or discourage increased use of computer-to-computer communications, with their very high data rates? Should charges be made on the basis of time or of the amount of information transmitted? Should heavy users over relatively inexpensive routes be required to subsidize users in remote locations that cost more to service? (That is essentially the present situation, whether for voice or data communication.)

2. Should the communications companies have a greater responsibility than they do now, to provide service with as few errors as possible? Or is it enough that they publish error characteristics of the various types of service and leave the user to make the choice that is most appropriate for him? If the communications companies are ever to be held responsible for errors in transmission, how could the blame be established and apportioned?

3. Would it be good or bad public policy if the computer manufacturers went in for communications gear and the communications people went in for computing services (such as selling unused computer capacity at off-peak hours)?

14. Computers and National Development

Background.—Most of the developing nations, often described as the Third World, are seeking actively to achieve levels of industrialization closer to those of Europe, Japan, and North America. We may hope that they will be able to imitate only our successes and not repeat our mistakes, but in any event it is clear that rapid development is their goal. With annual per-capita incomes of under $200 in many places, and with relatively trivial amounts of support coming from the so-called developed nations, development will be difficult since under these conditions it is hard to accumulate the capital needed for industrialization.

Questions

1. Is there some way that computers can help to accelerate the development process, substituting somehow for a part of the missing capital?

2. How should the developing nations seek to acquire the expertise needed to run successful computer operations? Through sending people to classes in the developed nations, and hoping they come back? By encouraging business arrangements that bring into the country experts who then spend much of their effort on training? By trying to use packaged programs to lessen the need for trained and experienced programmers?

3. Is it ever advantageous for a developing nation to try to build its own hardware? (Some people in the subject countries apparently would like to do so, somewhat on the model that says every new nation must have its own airline.)

4. What applications should be attempted first? Those that are the easiest and therefore most likely to be successful, or those that are most needed? (Only by good luck will these be the same.)

5. Is it wise for a developing nation to attempt macro-economic planning by computer, much as it may be needed, considering how difficult it is to do right?

6. To what extent will the rapid introduction of computers accelerate a trend toward homogenization of cultures, destroying local customs and traditions? (It is not always clear whether the nations in question want to avoid this process.)

7. Computer applications of greatest benefit to a nation with an annual per capita income of a few hundred dollars will probably not closely resemble those of a nation with an income of ten times that amount. Does this pose problems for the developing nations in deciding services, which then help them get bigger in a "them that has, they seek? Does it create difficulties for those in the developed nations who might wish to help the developing nations? Might it be possible to set up a kind of Computer Peace Corps?

15. Computers and Social Power

Background.—It has commonly been asserted that computers contribute to the concentration of economic, social, and political power. An (oversimplified) example of the concentration of economic power might be that the biggest institutions are best able to afford computing services, which then help them get bigger in a "them that has, gets" syndrome. (This is not an argument against bigness per se but an argument against unfair competition that bigness sometimes generates.) An example of concentration of social power might be the credit organizations' data banks, which apparently have great impact on people's lives. These existed before the computer, to be sure, but their present capabilities would be impossible without computers. An example of political power might be the disparity between the use of computers by the Executive and Legislative branches in the United States government, and the use of a computer by a well-financed candidate to generate mailing lists and "personalized" letters or to analyze neighborhoods to establish what each subgroup wants to hear.

Questions

1. Are the assertions above even true? There have always been imbalances of power and always will be. Has the advent of the computer really changed any of that, or has it just added another tool to techniques that were in use long before the computer era?

2. If they are true, even in part, what should be done about it? Should each candidate for national office be guaranteed by law to have access to a certain amount of computer power? It is hard to imagine how it might be done, but should small companies be granted a right to some of the power available to the big company? Or consider a regional planning association that is using computer modeling to guide its planning. Should it be public policy to require that countervailing groups be given access to the computing facilities, including the necessary programs, to test their assumptions?

3. If the concentration of power argument is accepted, what agency of society should police the efforts to equalize the imbalance? Trade associations? Major political parties? Congress? Professional organizations in computing?

4. If some equalization process should be decided upon, how would the security aspects best be handled? If the same computer firm is preparing voter mailing lists for both Smith and Jones, how are loyalties to be defined and policed?

5. In many important instances a computer in itself is of little value; what is important is the access to a large "data base" of information that could not be effectively processed without a computer. In other words, the computer and the data base, in these applications, would be useless without each other.

Many of the other problems considered in this report are of a like nature: in one sense the computer isn't really the issue, and yet the issue would never arise without a computer to make the application possible. How do we properly address such an issue in the context of "computers and public policy"? In one sense perhaps computer people have no "jurisdiction" since the computer is only an adjunct to the real issue, and yet if everyone defines his field of competence so narrowly the whole problem will fall into the cracks.

Perhaps this is just another way to approach the age-old puzzle about the degree of responsibility that the maker of a tool should have for its use.

16. Government Support of Computer Research

Background.—Government support has been heavily influential in the development of computers. For instance, punched card data processing equipment was developed for the 1890 United States Census, and one of the earliest electronic computers was dubbed The Defense Computer because its production was spurred by the needs of the Korean War. Many pioneering ventures over the years were either developed directly for military purposes, or financed at academic institutions with military or National Science Foundation support.

Questions

1. How much governmental support of computer research and development is desirable? Does financial support come with too many strings attached? Does governmental support carry the risk of distorting research priorities?

2. Without governmental support over the years, the computer field would be far less advanced than it is now. Most people in the computer field would probably find government support to be a good thing, on balance. Should support at such levels be continued in order to spur

further growth? If so, through what agency or agencies should it be channeled? How can effective pressure be brought to bear to obtain the needed support? On the other hand, some projects in the past have been much more productive than others. Can the evaluation of promising projects be strengthened?

3. Would government support of computing be more effective if it were decentralized, with less control being exercised by a few agencies?

EPILOGUE

These are some of the more pressing issues involving computers and public policy. It is not an exhaustive list, and it will change with time. Some of the issues will be dealt with in legislation that will be passed within coming months, and in that way they will be solved at least for the time being; others are not the sort of things that can be handled by law in any event, and will be of concern for many years. A similar list drawn up five years from now will no doubt contain a different set of issues, as some problems are resolved and new ones develop. This is to be expected in a new and dynamic field whose ramifications extend into almost all parts of society.

The hope in writing this paper is that, by clarifying some of the issues for a readership with a variety of backgrounds, faster progress will be made toward finding solutions that will benefit the most people.

Acknowledgment

Special thanks for valuable suggestions are due to J. Roger Hamilton, Laurence I. Press, Lawrence A. Rowe, Jean E. Sammet, Roger L. Shinn, and Margaret A. Wu.

Society, v. 12, March/April, 1975: 58-63.

The Technology of Surveillance

Technology has not only improved the intelligence data base, but it has done so with increasingly less provocation and fewer political risks.

by Herbert Scoville, Jr.

Beginning with World War II, technological methods of collecting intelligence have become increasingly dominant over the traditional agent, informer or defector as sources of information, particularly in areas affecting national security. Stealing plans, infiltrating agents into laboratories and visually observing new weapons have become more and more difficult and unproductive. Even if a spy succeeds in getting a look at a new weapon, he might not be able to acquire important information obtainable only with a scientific instrument. Thus, a person watching a nuclear explosion would learn little other than that it went off, with perhaps some estimate as to whether it was large or small; but a seismic instrument or an acoustic listening device halfway around the world could measure the explosive yield, and a filter in an aircraft at this same distance could collect particles from which the secrets of the internal design of the bomb could be determined.

Fortunately, as the usefulness of human beings for collecting intelligence has decreased, the science of technical intelligence collection has grown dramatically. Not only has collection technology improved, but modern military weaponry has made the task easier to accomplish in less provocative ways. Nuclear explosions release tremendous amounts of energy, and modern missiles travel along trajectories observable hundreds or even thousands of miles away. Radars and communications systems frequently bounce energy off the ionosphere so that the signals can be received at long distances. Modern weapons and their logistic support can be easily observed by aerial photography. As a consequence, available information on even the most secret military weapons and on the deployment of forces even in remote localities is far superior to what it was twenty years ago.

When President Eisenhower made his famous "Open Skies" proposal calling for unrestricted, but monitored overflight of national territories on both sides of the Iron Curtain, its acceptance would have gone a long way toward thawing the Cold War. The Russians disparaged it as legalized espionage. Today, thanks to technological improvements, our capabilities for obtaining military information far surpass any that we dreamed of under the Eisenhower plan and, surprisingly, the Soviet Union in the 1972 Strategic Arms Limitation Talks Agreements sanctioned the right of the United States to have pertinent military information, provided that it was obtained by national technical means not in violation of international law.

Communications Interception

One of the oldest forms of intelligence collection is intercepting communications. Early man undoubtedly watched hostile smoke signals and attempted to decipher the messages being transmitted. However, this form of intelligence collection took on new significance with the advent of radio communications, which not only heralded a tremendous increase in the volume of information communicated, but also presented valuable new opportunities for listening in on the messages being transmitted. Since such listening was so inherently easy, new countermeasures were developed to protect the privacy of radio communications. Encrypting messages became a standard procedure for disguising the content, and this, in turn, promoted a science of deciphering the codes. The race was on as one side attempted to improve the security of its communications system while the other side attempted to break through these barriers. Because this was a game of countermeasures and counter-countermeasures, dark secrecy was applied to efforts in this area. Successes had to be concealed in order to prevent them from being countered in future situations. The classic publicized case was the United States breaking the Japanese codes before World War II. The secrecy about this success was probably in no small part responsible for failure to take advantage of it at the time of Pearl Harbor.

Today, methods are available to make any specific communication invulnerable to being read. One-time cryptographic techniques make breaking specific messages almost

79-064 O - 76 - 36

impossible. However, in the real world there are practical barriers toward establishing such tight security on all communications would be needed between their various elenational security area, is so large that it is not possible to use such methods for every message. Furthermore, the operation of any system is always subject to human or mechanical errors and, in cryptography, these can lead to the compromise of information. To minimize this problem, resort is often made to land lines, short-range line-of-sight radio transmissions or reduction in the power of the transmitters in order to limit the opportunities for intercept.

Finally, even if a message is transmitted in an unbreakable code, intercepting the communication may still yield meaningful intelligence information. For example, the fact that points "A" and "B" are communicating is in itself useful datum since it shows some connection between the two points which could provide a clue about the nature of the work at "A" and "B." The activation of communications links between a missile launch site and a missile impact point would be an important indicator that a missile might shortly be fired. Since these types of communications could provide clues to the hordes of analysts involved in communications intelligence, communications security must go beyond establishing codes. Security must control the volume and nature of the traffic on any communications link, and frequently pass false messages in order to hamper traffic analysis.

Intercepting communications can provide a wealth of useful information on governmental plans and thinking. Different sections of a modern bureaucracy must communicate to operate. While the most sensitive messages can be kept secret, many of the less critical ones can be intercepted and understood. Furthermore, much useful information must be transmitted completely in the open, and, occasionally, this can be of vital importance. For example, at the end of August, 1961, a woman listening to open radio transmissions within the Soviet Union at a receiver in the eastern Mediterranean heard an advance press release with a three-day embargo announcing that the Russians would resume nuclear testing. She recognized the significance of this message, pulled it out of the mass of transcripts which were being made routinely and forwarded it by priority to Washington. This unclassified message notified President Kennedy in advance of Soviet intentions to terminate the nuclear test moratorium, and provided the opportunity to take political action to forestall the Soviet move. Unfortunately, the government decision-making bureaucracy was too cumbersome and, in the end, the President docilely allowed the Soviets to recommence testing. Thus an important political opportunity was lost.

The usefulness of communications intercept in the national security field is so great and all-encompassing that the selection of specific examples can be misleading. Almost all military activities in peacetime and in war depend heavily on communications. If these can be read, then national security would be greatly enhanced. In the event that military forces were to be used in a surprise aggression, widespread communications would be needed between their various elements. The understanding of even one of these messages might give advance warning and eliminate the surprise. It could be the difference between national survival or collapse.

While the communicator normally must send thousands of messages, the intelligence collection system might break the code with a single success. Even if the content of the messages cannot be read, the increased volume of communications could frequently be the indication that some operation is imminent. Communications between military aircraft and the ground are an important source of intelligence on military operations. In the heat of battle, communications security is frequently very poor.

As mentioned previously, messages passed on a missile test range or at other weapons test sites can provide important clues to the nature of the weapons system involved. For example, at the Atomic Energy Commission's test sites in Nevada and Eniwetok, scientists were in constant communications between various instrumentation stations and the laboratories at headquarters. Although there were strict injunctions on communications security, any recording of these messages would certainly have provided invaluable information on the nature of the tests and their results. Security had to rely primarily, but not always successfully, on the fact that the frequencies and power used in the communications system were such as to limit the range over which they could be received.

As technology has improved, however, the ability to pick up weak signals, to use computer techniques for pulling information out of the noise and to understand better the nature of an anomalous radio transmission has made it easier to overcome attempts to conceal the messages. Computers are also critically important for cryptoanalysis, although never sufficient to break a truly first class communications code. The countermeasure/counter-countermeasure battle continues today, albeit at a much higher technological level.

What are the political implications of intercepting governmental communications? All countries now take for granted that attempts are being made to intercept their communications, and employ the best countermeasures of which they are technically capable. However, this works to the disadvantage of less affluent and less developed countries since they do not have the resources or the sophistication to carry out such operations on a sufficiently extensive scale.

The provocation from this type of operation depends primarily on the means and location by which the intercept is carried out. Much can be done from international waters or from friendly countries bordering the target area. In the latter case, political sensitivities can be raised since most nations do not wish it known that their territory is being used as a base for intelligence operations against their neighbors. However, such operations are so widely practiced that they now are rarely the cause for international protest. The use of a friendly country as a base does create a degree of indebted

ness to that country, which could be a political liability. We are prone to support regimes which allow us to use their territory even though the objectives of that regime may not be compatible with our basic political goals. This problem applies to cooperation in intelligence gathering generally, and is probably less serious in communications intercept than in more clandestine or provocative operations.

For some types of communications, receiving at a distance is impractical, and this leads to operations which can be much more provocative. For example, to intercept certain air defense communications, it may be desirable to fly very close to the border. Occasionally, errors can occur in which the aircraft accidentally overflies another nation's territory. This can cause major incidents. Even more provocative would be a situation in which the aircraft purposely intruded across the boundaries of a country, but this rarely occurs any more; certainly not by the United States over Russia or vice versa. However, both countries may have covert communications intercept operations inside the other nation's borders, possibly for the purpose of intercepting a highly sensitive communication link unobtainable at long range. Such an operation, of course, has all the political risks of any covert operation and would only be practiced under highly critical situations.

A new form of communication employs satellites as relay stations. Since these transmit over very long distances, they are intercepted easily without need for provocative collection operations within the territory of the communicating country. In general, such highly sensitive messages would not be transmitted over satellite unless some unbreakable code were used.

Electronic Intelligence

Similar technological intelligence collection involves the intercept of radio waves of a non-communications type, particularly those from radars. This type of intercept, known as "ELINT" (Electronic Intelligence), first came into being with the advent of radar in World War II, and has since blossomed into an extensive intelligence activity. In addition to detecting and tracking hostile aircraft and missiles, radio beams are used for guiding defensive missiles toward the incoming targets. Although many modern offensive missiles now rely on inertial or laser guidance techniques to avoid possibilities of jamming, radars are often used for offensive missilery as well. Radars are critical to all manner of naval operations. Thus the collection and analysis of ELINT has become a very high priority task of all military intelligence organizations.

Radars, if they are to be of any military use, must be continually exercised. An air defense radar which is not turned on provides no defense at all. Furthermore, training must be continuously carried out to insure that they are operated properly. All of these factors provide frequent opportunities for carrying out ELINT operations. Countermeasures, such as with the coding used for communications transmissions, are not available to maintain security. The only protection is to restrict the operations of the radars to locations well within the interior of the country so that the opportunities for ELINT collection are minimized. However, even this is not feasible since most air defense radars must be located near the border, aimed out, in order to detect aircraft flying in. The same is true for ballistic missile defense radars. Moreover, even for tactical electronic equipment, maneuvers must be carried out, and, particularly in Europe where the most advanced systems are likely to be employed, these must be held in regions susceptible to observation by foreign intelligence.

All countries now take for granted that attempts are being made to intercept their communications.

However, despite the increased opportunities for ELINT collection, all such operations are not necessarily nonprovocative. In order to detect anti-aircraft radars located along the periphery of a country, it is frequently necessary to fly aircraft and sail ships close to the borders in order to intercept the signals. Frequently, such operations are subjects of international incidents. The *Pueblo* seizure off the coast of Korea is an example of one in which the intercept platform, this time a ship, was seized in international waters, although operating in a perfectly legal manner. On another occasion of more doubtful legality, a United States RB 47 flying along the Russian arctic coast was shot down and the crew captured in 1960. The United States insisted that the plane was always over international waters, but the Russians claimed it had penetrated into their air space. When the crew was returned as part of the detente at the begining of the Kennedy Administration, the crew members admitted having been over Russian territory, thus partially substantiating the Russian claim.

Even when over international waters, such operations can be provocative and are often a potential source of international incidents. In order to insure that the radars will be turned on and functioning in a truly operational mode, the aircraft frequently approach the coast as if intending to penetrate the national boundaries. It is not surprising that under such circumstances, trigger-happy air defense personnel are inclined to take counteraction. Furthermore, the scale and number of such operations is probably much larger than can be really justified on the basis of military need. There is always a tendency in such a situation to repeat operations, consequently increasing the probability of an incident. Greater restraint on the part of those authorizing such operations would probably reduce international tensions without any serious loss to national security.

A related type of intelligence collection normally classed

under ELINT is the intercept of telemetry signals from new weapons testing programs. In order to develop a new missile or carry out a space mission, a nation must equip its test vehicles with instrumentation to measure the functioning of various components, and the only way in which the data from these instruments can be relayed back to the test site is by radio-telemetry. Since in many cases the telemetry signals will be receivable at long distances from the source, the opportunities for intercepting such signals outside the country are great. Interpretation of the signals may be more difficult than for the nation originating the telemetry, but, nevertheless, useful information can frequently be obtained on the nature of the test program.

An example of conspicuously successful telemetry intercept occurred at the time of the first Soviet manned space flight. United States receivers in the Aleutians were able to pick up the television pictures of the astronauts as they were being transmitted back to the Soviet Union so that United States authorities knew simultaneously with the Russians that the mission was a success. Soviet secrecy had led to considerable skepticism over their claims of space superiority, and these intercepts provided the data for an independent analysis of their achievements.

Since most of this collection can be carried out at long distances and outside the territories of the testing country, it is not provocative and therefore not a source of international friction. Truly covert ELINT operations within the country are rarely needed or feasible, but in some areas, the territories of friendly countries are required as a base of operations. This could lead to political embarrassment and an undue dependence on the goodwill of that country in order to obtain permission for the operations. A case in point is Turkey, which is strategically located opposite the southern border of the Soviet Union, where much of the Soviet missile-launching and other weapons testing occurs. It is no secret that the United States has many stations in that country for the collection of such information, and the continuance of these operations is dependent on maintaining good relations with the Turkish government. These relations were recently subject to strains as a result of our desire to persuade the Turkish government to halt the cultivation of poppies, a major source of the illicit drug trade in the United States. The United States could have been hampered in its representations to Turkey by the desire to keep these strains from reaching the point where receiving sites would be lost there.

Radars for Intelligence

A final form of electronic intelligence collection is the converse of ELINT, the use of active radars to observe a missile in flight. This type of collection, known as "RADINT" (Radars for Intelligence), involves the transmission of easily detectable radio signals so it cannot be done clandestinely. It has been used very successfully to observe missile flight testing by operating high-powered radars within line-of-sight of the ballistic missile trajectory. By this method, the United States was able to confirm the first Soviet Intercontinental Ballistic Missile test flight in 1957, and to keep track of virtually all launchings of long-range missiles since that date. The deployment of such radars on native territory is of course non-provocative since radiation has no effect on the object in space. However, as in the case of the telemetry receivers referred to earlier, the radar had to be located in Turkey in order to observe the launch ends of the Soviet medium, intermediate and intercontinental range ballistic missiles.

Although there was a moderate amount of secrecy associated with this radar installation to avoid undue provocation, it could not be kept from the Russians since it was a large installation transmitting very powerful radio waves. As far as is known, no official protest was ever made to Turkey over this installation. However, it did increase United States dependence on Turkish goodwill. The more that type of technological intelligence collection is recognized internationally as legal, the less will be the dependence on the goodwill of the nation for its continued deployment. The United States and the Soviet Union have now endorsed such national technical means for use in verifying arms control agreements.

Ever since the first nuclear explosion, an important intelligence goal has been to acquire knowledge of foreign nuclear tests.

A new form of RADINT which can perhaps become of increasing value and which would present even fewer international problems would be the use of "Over The Horizon" radars. Since these do not require line-of-sight location, they do not need to be located in sensitive areas. However, at present, such technology is not as advanced, so that the quality and thus the value of the information gathered would probably be considerably lower.

Nuclear Test Detection

A special class of technical intelligence techniques includes those devised specifically for detecting and obtaining information on nuclear tests. Ever since the first nuclear explosion, an important intelligence goal has been to acquire knowledge of nuclear tests carried out by foreign governments, and, insofar as possible, to gather as much information on the nature of the explosive used. As a consequence, over a period of years, a series of highly sophisticated scientific methods were developed and put into operation.

These specialized techniques included seismic and acoustic receivers which could pick up the shock waves transmitted through the earth and air and provide data on the location and size of the explosion. Recordings of the electromagnetic waves produced at the moment the explosion occurred provided supplementary information. For detonations which took place in the atmosphere or which vented into the atmos-

phere, the collection of the radioactive debris provided unequivocal evidence that it was indeed nuclear in origin, and, most importantly, information on the nature of the explosive device. All of these techniques were refined until a very sophisticated intelligence collection system emerged and made the nuclear programs of any nation testing in the atmosphere relatively open. Since 1963, all tests except those carried out by France and China have taken place underground so that detailed information available from radioactive debris analysis has been denied.

Since very small amounts of radioactive material are needed to carry out detailed radio chemical analyses, the debris does not need to be collected close to the source. Aircraft flying over international waters and, in many cases, on the opposite side of the world, are quite satisfactory for sampling the bomb clouds. Thus, this very useful intelligence technique does not involve any provocative action. Occasionally, bases from which the sampling aircraft take off were located in foreign countries in order to obtain cloud samples within a shorter time after the explosion, but the use of such bases has never generated any international repercussions. Overflight of non-friendly nations was never required.

Photoreconnaissance

While all the foregoing technological methods of intelligence collection are extremely useful for the maintenance of adequate information to protect our national security, they are dwarfed in importance by photoreconnaissance. A picture is worth a thousand words—and often many reels of recorded radio signals. Photography provides easily understandable evidence even when a skilled photo-interpreter is needed to describe the object on the film. It has applications in almost every intelligence area, whether it be scientific, political, economic or military.

While photoreconnaissance has long been an important tool of intelligence, recent technological advances culminating in the capability to obtain useful photography employing satellites as platforms have completely revolutionized the entire intelligence collection process. No longer can any nation hide its military and industrial activities behind an Iron Curtain. The mission of an agent to procure information on troop dispositions, missile deployments or submarine construction has now been eliminated. An entire country can be photographed within a few days, the only limitation being the degree to which clouds interfere, and almost no area in the world is continuously cloud-covered. Thus, with persistence, any target is now subject to photo observation.

Aircraft photoreconnaissance has tremendous value in some situations since the vehicle can be easily directed on short notice to a specific location, can take a high resolution picture and can give a planner usable information within a few hours after the return of the plane. It has the disadvantages of the need for a base within range of the target, of limited area coverage, of vulnerability to destruction and, most importantly, of being extremely provocative. It is hard to tell whether a plane is carrying a camera or a bomb. This hostile characteristic frequently destroys completely its value as an intelligence tool in peacetime. Because of their flexibility, aircraft will probably continue to have limited utility as platforms for photoreconnaissance despite these drawbacks.

The fourth of October, 1957, marked the beginning of a new era, which culminated in the current revolutionary improvement in capabilities for photoreconnaissance. On that day, the Soviets orbited their first satellite, which traversed the United States and many other countries of the world and set the precedent for making legitimate space transit of national territories without permission of the states involved. No request was ever made for permission to carry out this operation, and no complaint was ever voiced by the Soviet Union when the United States followed suit the next year. No other country has ever raised the question of legality, and thus the first steps were taken toward the establishment in customary international law of the freedom of access to outer space for peaceful and scientific purposes.

Early Space Flights

Of course, these early satellites did not contain any cameras for taking pictures of the territory over which they passed, but the precedent had been set, and it was not long thereafter that at least crude reconnaissance capabilities became available. In 1960, the United States orbited weather satellites capable of making photographs which could define large geographical features such as lakes, but not smaller manmade objects such as buildings or vehicles. In April, 1961, the Soviets placed Astronaut Gagarin in orbit around the earth so that at least limited visual observation would have been possible. Still no complaints on the part of any nation. Admittedly, these early space flights were of no practical value for intelligence purposes, but they did help set the stage for international approval of satellite reconnaissance.

Already by May, 1960, when the U-2 aircraft was shot down over the Soviet Union, the United States had foreseen the eventual demise of aircraft reconnaissance over many foreign countries and had proceeded with a program for developing methods of obtaining similar information from satellites. The Soviet Union paralleled the United States' development of observation satellites, and both nations improved the capabilities of their systems throughout the 1960s.

By 1964, Secretary of Defense Robert McNamara was regularly reporting publicly on Soviet strategic deployments, and in 1967, President Lyndon Johnson extolled the virtues of the United States space program for protecting our security. In recent years, Secretaries of Defense Melvin Laird and James Schlesinger have described the Soviet strategic posture in detail, frequently announcing new construction very shortly after it began and accurately describing the size of Soviet missiles. Neither country, however, publicly admitted the method by which this information was obtained in

order to avoid a political confrontation and a possible international uproar which might have raised questions as to the legality of such operations. Instead, there was a tacit recognition of photographic satellite capabilities by both sides and perhaps an increasing realization that the availability of the information to the other nation provided a stabilizing influence.

Satellite reconnaissance has a number of major advantages over that carried out by aircraft in addition to its invulnerability and international acceptance. A satellite in an orbit of 100 to 300 miles altitude can survey large areas in a short time. If a satellite were launched in a north-south polar trajectory, then the entire earth could be covered, once in daylight and once at night, every twenty-four hours. Thus, a satellite camera platform is ideally suited for searching large areas to determine the presence of military equipment and installations. Apparently, at the present time, the United States and the Soviet Union each have systems that can rapidly photograph large areas as well as those that can focus on specific locations deemed of interest as a result of large area surveys.

In the early 1960s, while the early reconnaissance satellites were being gradually improved, debate was simultaneously proceeding on the international legality of such operations. Although the principle of free access to space for peaceful purposes was universally recognized from the outset, considerable debate ensued concerning the definition of the term "peaceful." In 1962, in the Legal Subcommittee of the United Nations Committee on the Peaceful Uses of Outer Space, the Soviet Union proposed that the "use of artificial satellites for collection of intelligence information in the territory of foreign states is incompatible with the peaceful objective of mankind in its conquest of outer space." The United States, while not accepting that reconnaissance satellites were "incompatible" with the peaceful uses of space, was, nevertheless, a strong advocate of restricting the use of outer space to non-military purposes. This apparent inconsistency in position was clarified by a later United States statement that reconnaissance was non-aggressive and, therefore, should be considered peaceful and essentially non-military. The United States argued that observation from space is consistent with international law as is observation from the high seas.

Treaty on Outer Space

This difference in point of view between the United States and the Soviet Union was finally resolved in the fall of 1963 when the Soviet Union suddenly dropped its insistence on including a ban on space reconnaissance and negotiated with the United States representatives a United Nations resolution dealing with outer space. The resolution called upon all States to refrain from placing in orbit nuclear weapons or other weapons of mass destruction. The United States and the Soviet Union had just previously stated their intentions not to do so without including any reference to the issue of reconnaissance satellites. This public change in Russian attitude may have resulted from their acquisition of a satellite reconnaissance capability of their own, although Nikita Khruschev was reported to have stated earlier that satellite photography was permissible. In 1967, this United Nations resolution was broadened into a Treaty on Outer Space, which carefully omitted reconnaissance from the banned activities. However, no document during this period ever specifically endorsed the use of space for reconnaissance purposes.

The final seal of approval was placed on the use of space for photoreconnaissance by the Anti-Ballistic Missile Treaty and the Interim Agreement on Offensive Weapons signed in Moscow in 1972. In these agreements, the United States and the Soviet Union agreed that national technical means should not only be used to verify the provisions of these arms control agreements, but also that these information collection

Politically risky agent operations should not be carried out if the increment to data from technical methods is not large.

methods should neither be interfered with, nor have deliberate concealment measures used against them. While satellite reconnaissance is not specifically mentioned in the treaty, the legislative history is clear that this was the key method of information collection referred to. While these were bilateral agreements between the United States and the Soviet Union, no other country has ever objected to such reconnaissance, and thus one can say that it now has widespread international legality. At last we have available a technological intelligence collection tool which is recognized as legal and, therefore, non-provocative. Since such reconnaissance is capable of satisfying a wide variety of information needs, it should reduce the justification for intelligence collection by more provocative methods.

Technology has not only improved the intelligence data base, but it has done so with increasingly less provocation and fewer political risks. But have national security planners and the intelligence community taken this new situation into account adequately? Politically risky agent operations should not be carried out when the increment to data available by technical methods is not large. Provocative peacetime aircraft missions are unnecessary when satellites can provide the same data (even if the latter method is more expensive). The United States should not negotiate arrangements with governments inimical to democratic principles just to obtain a base for redundant information available from other sources. Aircraft and naval missions which run the risk of armed conflict should be carefully reexamined to determine their real priority. Some of these changes are undoubtedly taking place and may be behind the reported cutbacks and reorganizations in the intelligence community, but in light of revolutionary improvements in the technology of intelligence collection, more old methods should be retired.□

94TH CONGRESS
2d Session
SENATE
REPORT
No. 94-755

SUPPLEMENTARY DETAILED STAFF REPORTS ON FOREIGN AND MILITARY INTELLIGENCE

BOOK IV

FINAL REPORT

OF THE

SELECT COMMITTEE
TO STUDY GOVERNMENTAL OPERATIONS

WITH RESPECT TO

INTELLIGENCE ACTIVITIES
UNITED STATES SENATE

APRIL 23 (under authority of the order of APRIL 14), 1976

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1976

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price $1.90

LETTER OF TRANSMITTAL

On behalf of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, and pursuant to the mandate of Senate Resolution 21, I am transmitting herewith to the Senate two detailed staff reports which supplement Book I of the Committee's final report, entitled Foreign and Military Intelligence. In addition, this Book contains the addenda to the Committee's Interim Report on Alleged Assassination Plots and a composite of written interrogatories submitted by the Committee to former President Richard M. Nixon and his responses.

The turbulent history of the past 30 years is closely bound to reasons for the growth and evolution of the intelligence functions in the United States Government. The first study in this volume is an unclassified history of the Central Intelligence Agency. It is published to assist the Congress and the people of the United States to better understand the nature and character of the intelligence activities undertaken by their government. It is also intended to assist those who must make judgments about the necessity for intelligence activities by the United States in the future. The Select Committee is grateful for the assistance given by the Executive branch to the Committee in the preparation of this historical study.

The second study contained in this volume, "Intelligence and Technology", was written by Dr. Richard Garwin, a distinguished scientist who has served the Select Committee as a consultant. It was prepared for the Committee in order to enable the Congress to understand the potential threats that intelligence technology can create for the rights of U.S. citizens. Successor committees will have the task of drafting charter legislation for the intelligence activities of the United States Government. This essay is intended to provide a glimpse into the future of intelligence technology so that in the drafting of new laws there could be a sufficient awareness of intelligence technology to make sensible balancing judgments between the needs of intelligence and the rights of American citizens guaranteed by the Constitution.

Once again I want to acknowledge the great effort, dedication, and talent of the Committee staff. Finally, I want to express the deep appreciation of the Committee to Senator Walter D. Huddleston for his work as Chairman of the Foreign and Military Intelligence Subcommittee and the work of the other Subcommittee members, Senator Charles McC. Mathias, Senator Gary Hart, and Senator Barry Goldwater.

FRANK CHURCH,
Chairman.

INTELLIGENCE AND TECHNOLOGY[1]

I. Background

The First Amendment right to free speech and the Fourth Amendment right to be secure in one's person, papers, and home have been violated in recent years. Although these rights have been abridged in time-honored ways, in some cases the abridgement has taken place in ways that could not have been foreseen by the framers of the Constitution and the Bill of Rights. A partial list of means employed follows:

Breaking and entering into offices and homes;
Opening of letters in the Postal System;
Bugging or use of hidden microphones with no party to the conversation witting;
Wiretap of telephone communications;
Intercept of telephone communications without actual connection to wires; and
Intercept of facsimile or printer communication.

Although files have existed for many years in all societies, and have sometimes been used to pernicious ends, technology has now made available to the managers of personal files greater speed and efficiency in the retrieval of data, as it has to managers of inventory files, of airline reservations, of the corpus of legal decisions, and of the United States House of Representatives Computer Based Bill Status System. In recent years, too, heightened public sensitivity and legislative activity have begun to introduce legislation, guidelines and standards regarding governmental and private files on individuals, granting the individual in many cases the right to know of the existence and the content of such a file, and to be able to challenge information which may be found in that file (Privacy Act of 1974, 5 U.S.C. 552A). Computer technology may not have been instrumental in the misuse of CIA or IRS files to provide information to the White House on U.S. citizens, but the future impact of such technology must be assessed.

It is a logical possibility that the modern technological tools employed in the exercise of other rights and freedoms for the general and individual good might inadvertently result in such general exposure that the First and Fourth Amendment rights could no longer be preserved, or that their preservation would require severe restriction of other rights and freedoms with major damage to society. For example, such might be the impact of (fanciful and unphysical) spectacles which, while restoring perfect vision to older people, endowed them as well with the ability to look through envelopes and walls.

A second logical possibility is that the general exercise of technology for individual good and the good of society does not in itself imperil the rights under discussion, but that specific targeting of this technology toward individuals can imperil these rights. In this case, the particular threat to these rights could of course be removed by outlawing the subject technology and enforcing such laws. It may be,

[1] This staff report was prepared for the Select Committee by Richard Garvin, consultant.

however, that comparable protection of these rights may be obtainable by legal restrictions on the *use* of such technology, for such invasion, without denying society benefits which would otherwise be obtainable. If similar guarantee of rights may be achieved in this way, the banning of technology (even if politically feasible) would be an exaggerated remedy.

Finally, in some cases new technology may aid in restoring privacy against invasion by people or tools. An old example is the use of locks on doors; newer ones are the use of encryption for written communications and for the privacy of information in files. On the other hand, it would be inappropriate to require the individual to go to great cost to preserve his rights if such preservation could be obtained at lesser social cost, *e.g.* by restrictions of the actions of individuals who would intentionally violate these freedoms or whose activities might inadvertently imperil these rights. Thus, the expectation of privacy for the contents of a post card sent through the mails is quite different from that of a first-class letter in a sealed envelope, and the cost of an envelope is not regarded as an excessive charge for the guarantee of privacy. As the human senses and capabilities of vision, hearing, and memory are expanded by the use of new tools, what is the place for the analog of better envelopes?

II. Covert Observation and Intercept

Covert hearing (hidden microphones).—It has always been possible for a person to secrete himself, unbeknownst to the participants in a conversation, in such a way as to hear the conversation and so to violate an expectation of privacy ("eavesdropping"). No doubt mechanical aids in the form of tubes were used at times to make eavesdropping easier and less dangerous. Furthermore, rooms equipped with speaking tubes to convey orders to another part of a building were vulnerable to another kind of eavesdropping in which the use of the apparatus was other than that intended.

Microphones were in use in the 19th century for telephone communication and more recently for radio, public address, and recording. The present state of microphone technology is apparent to us all, with microphones a few millimeters across and a millimeter thick common in portable cassette recorders in use for business, education, and pleasure throughout the world. Over the last few years, the development of integrated-circuit technology and its extremely wide use in such recorders, in stereo equipment, and in calculators has provided not only the possibility but also the widespread capability to house amplifiers in a space of a few cubic millimeters and with power consumption of microwatts. Thus, microphones can be hidden in walls or moldings of rooms, in furnishings, or in personal possessions. They can be left behind by visitors or can be introduced as part of the normal resupply or refurbishment process.

Microphones can be accompanied by self-contained recorders or can transmit the signal (usually after amplification) either along near-invisible wires or by radio. In the case of wire or radio transmission, there would normally be a recorder or more powerful relay at some small distance of a few meters to a few hundred meters. The power requirements for microphones and amplifiers can be provided by batteries, by connection to the normal building power supply, from the

telephone system, or by silicon or other cells converting sunlight or roomlight into electrical power. Microphones can also be provided with power by the absorption of radio or microwave signals, and can retransmit intelligence on the same carrier waves. In addition to dedicated wires or radio transmission, the microphone signal can also be transmitted on the building power line or on the telephone lines, if any. Under most circumstances, the ability with further advance of technology to make microphones still smaller would not be of great utility. They are already small enough to pose a near-maximum threat.

Not only are apparatus containing microphones available by the tens of millions throughout the world, but the components are also common articles of commerce and can be assembled by any one of millions of people. Many rooms are now permanently equipped (entirely overtly) with microphones for use in recording conferences or in picking up clearly comments made by an audience during question period. Such microphones could easily feed recorders, wires, or transmitters at other times as well. Furthermore, every loudspeaker, whether built-in or part of a portable electronic device, is capable of working as a microphone in just the same way. Individuals with impaired hearing have particularly small microphone-amplifiers, some of them concealed in the frames of eye glasses.

A slightly different kind of covert hearing is said to be possible by detecting with laser beams the vibration of ordinary windows enclosing a room in which the target conversation is taking place. Another approach to overhearing conversations outdoors is to use large directional microphones distant as much as one hundred meters.

Retarding the further development of microphone technology for commercial purposes would be of little help, even if it were feasible, given the already small size of microphones. It seems likely that privacy can be adequately protected against covert hearing in the United States by proper legislation and enforcement requiring a warrant for the exercise of covert hearing capability. There being no expectation of privacy against a person present, legislation in the future, as now, should not restrict covert recording or retransmission by a person present, whether that person participates in the conversation or not. Of course, covert hearing capability can be banned administratively from designated premises, as it is now, by those in control of the premises—*e.g.*, "no microphones, radios, recorders, etc. at defense installations" (or on premises operated by the XYZ company).

Covert seeing (hidden cameras).—Hidden cameras (whether electronic or film) can imperil Fourth Amendment rights in analogous fashion to hidden microphones. Observation through a crack or peephole; personnel observation via a partially transparent overt mirror; large automatic or remote-control cameras or TV-type sensors behind an overt mirror; small cameras behind a small aperture—this series represents the application of technology to the goal of covert seeing. Vision comparable with that of a person can be obtained through a hole about 3 mm (⅛-inch) in diameter. A 1 mm hole would permit commercial TV-quality picture. Reading the text of papers on a desk across the room will require a larger aperture. Unlike microphones, such cameras are not yet common or cheap. A film camera taking a picture every 5 seconds would need a considerable film supply and would have to be quiet if covert; a TV camera capable of communicating even

at such a rate, with human vision quality is feasible, but is at present costly. With time, the technology of fiber-optic signal communication will allow unobtrusive relay from a hidden camera. A command link could direct the view of the camera toward the interesting portion of the room, saving power and communications rate (as could built-in intelligence at a later time).

Clearly, the invasion by covert seeing of privacy would be intentional, not the result of innocent exercise of rights on the part of others. As such, preservation of such privacy can look toward legislation and the enforcement thereof, with such unconsented observation available only under warrant.

Wiretap of telephone lines.—Anywhere on the line running from the telephone instrument through the building to the junction box and on to the local exchange (typically a mile or so from the subscriber's instrument), connection to the line or proximity to that line will allow a high-quality telephone conversation to be provided for listening or recording. For many decades there has been no need for physical contact with the line to allow "wiretap," and no telltale click or change in quality is necessary or likely.

The technology needed for wiretap (whether by contact or noncontact) is primitive compared with that used for covert hearing. There is no way in which this technology can be outlawed without outlawing telephones themselves. However, in this field particularly, there is no necessity to abandon the protection of privacy. The intercept of communications from telephone lines may readily be controlled by legislation and by the requirement of a warrant for such actions by government bodies.[14]

Intercept of voice from domestic microwave relay.—In the United States, most telephone calls beyond the local area are now transmitted via microwave relay. Towers about 20 miles apart contain receiving antennas, amplifiers, transmitters, and transmitting antennas. The microwave relay system operates near 4000 megahertz and 6000 megahertz, at wavelengths on the order of 6 centimeters.

The transmitted beam from each of these relay towers has an angular width on the order of one degree and so can be picked up well over a wedge some 20 miles long by a third of a mile wide. Leased-line services such as the federal government FTS system, WATS lines, and individual corporate "private-line" networks occupy permanent positions in the frequency spectrum in those relays which are used to carry the signals (not always by the most direct path) over the fixed network. Direct-distance-dialing calls, constituting the bulk of the traffic, cannot be so precisely located. In general, however, these DDD calls are preceded by digital information which serves to direct the call to the receiving telephone number and to indicate the calling telephone number as well.

At present, an individual with an instruction manual and a few thousand dollars worth of equipment can set up a makeshift antenna and listen or record continuously calls on any desired fixed-assigned channel. In principle, even the DDD calls could, at substantially larger investment, be matched with a list of "interesting" telephone numbers

[14] Omnibus Safe Streets and Crime Control Act of 1968 (18 U.S.C. 2510–2520).

so as to record only those calls originating from or directed to a given subscriber number.

These voice messages, having traveled by wire at least some distance may be from the telephone instrument, legally afforded the same protection as calls carried on wire from sendor to receiver.[2] However, questions of extra-territoriality arise. There appears to be no way in which individuals on foreign embassy and consular properties can be forbidden from listening into those microwave links which pass their territories. It must be anticipated that certain powers will use such information not only for affairs of state,[3] but also simply to earn funds by taking advantage of information which is obtained in this way. Communication in regard to commodity markets, stock exchanges, and bidding prices for large contracts all convey information which can have substantial value.

Given this peculiar situation, one might judge that the threat to privacy from all but extra-territorial intercept is adequately controllable by a legislative ban on such intercept (and the requirement of warrants for government "search"), and that the rather limited exposure to personnel controlled by foreign powers and based outside the reach of U.S. law can be controlled by other means. Voice links carrying defense information are all encrypted. Other important information of the federal government can be rerouted to avoid some small number of possible listening posts. Direct-distance-dial calls eventually will be relayed with the destination and origination information going over separate channels. When all-digital transmission is used to carry voice, encryption can be available at negligible cost. It could be implemented with separate keys for each microwave link, or encryption could be done at the point of digitizing each signal, or both.

Intercept of non-voice from domestic microwave relay links.—Many channels on U.S. microwave relay are devoted to the transmission of non-voice information (facsimile machines, teletype, telex service, other printer traffic). The comments above regarding the intercept of voice communications from such microwave links apply with equal force to the intercept of non-voice communications. There is, however, a major difference. Existing law protects only communications from which intelligence can be "aurally acquired," [4] so there is at present no legal bar to the intercept of such non-voice communications.

At present, the value of the average non-voice communication relayed over the microwave net is probably greater than that of the average voice communication. Even if non-voice were protected by new legislation, it would still be subject to intercept from extraterritorial sites. Fortunately, the protection of non-voice data transmission by means of encryption is far easier than is the case for voice and is practical now over all telex and printer links. Several machines and electronic devices of varying effectiveness are available to provide end-to-end transmission security. The National Bureau of Standards

---

[2] 18 U.S.C. 2511.

[3] Report to the President by the Commission on CIA Activities Within the United States. June 1975, p. 8.

[4] 18 U.S.C. 2510(4).

has begun the promulgation of a national standard for data security via encryption, which apparently satisfies the concerns of the United States Government for maintaining the privacy of non-defense information.

Intercept of voice or non-voice from domestic communication satellite links.—About half the international common-carrier communications originating in the U.S. goes by satellite and half by submarine cable. A rapidly increasing fraction of purely domestic communications is now relayed by satellite. Present satellites may receive communications from any one of a number of ground stations and simply rebroadcast the signal at a different frequency, covering the continental United States with the microwave beam. For some communications with multiple addressees, this large potential receiving area is an advantage; for most communications with a single addressee, the particular ground station to which the message is addressed will recognize the digital address and record or retransmit the message into the local net (or print it and put it into an envelope for delivery, etc.).

Modern relay satellites are in stationary orbit, so that a fixed antenna can be used to receive signals, rather than the tracking antenna initially required for the lower-orbit satellites. Thus, anywhere in the large area illuminated by the satellite microwave beam, a relatively simple antenna and amplifier would allow intercept of messages relayed by satellite. The satellite transmits microwave energy not only onto the land mass of the U.S., but also onto adjacent waters and countries, including Cuba. Non-U.S. citizens on non-U.S. territory are completely free to receive satellite relay of domestic U.S. communications and to do with this information whatever they will.

Although some satellite relay is digital in nature and thus readily protected by encryption at negligible added cost, the voice communication is primarily analog (whereby the intelligence is carried by continuous amplitude or frequency modulation as is the common case for terrestrial multiplex relay). Encrypted voice communication would require a wider channel at present than is needed by analog voice, but the additional cost for privacy via encryption might be small even so, since the satellite resource is a small part of the end-to-end communications cost.

Unfortunately, domestic satellite relay, as presently practiced, is an example of a case in which the indisputable benefits of technology bring with them a threat to privacy. In this case, it is not the application of technology to intercept but the technological nature of satellite transmission which makes intercept as easy outside U.S. territory as within, thus putting protection of privacy outside the reach of U.S. law. Technology in the form of encryption provides an adequate solution. This remedy is available now for non-voice communication and could be used with equal ease for digital voice. Aside from encryption, satellite voice communication could be provided some degree of protection in the near future by avoiding fixed-assignment schemes for users desiring privacy.

III. File Technology

Some examples of current status.—Among the early large computerized file-oriented systems were the airlines seat reservations systems now in use by all U.S. airlines. The overall system accommodates thou-

sands of flights per day, with a hundred or more seats per aircraft, and can handle reservations months in the future. A reservation can be made, queried, or cancelled within seconds from many hundreds or thousands of terminals. Some of the records may contain little more than the name of the passenger; others may include a complex continuing itinerary, with hotels, car rental, telephone numbers, and the like.

Seismic data bases are used by oil exploration companies to hold seismic reflection data and core logs. The former is the pattern of reflected sound waves versus time at various microphones which are sensitive to signals from a small explosion at the surface of the ground. The reflection comes from change of structure at different levels in the earth below. Core logs (or bore logs) may measure the detailed ground conductivity, water content, radioactivity content, and the like in tens of thousands of oil exploration wells. The material is kept computer accessible so that it can be retrieved and processed in a timely fashion as new tools are developed or as new information makes it desirable to compare with old information in the neighborhood.

Several government echelons have tax data bases. At the city or county level, such a data base may include details about every dwelling in the city. Such data bases can be particularly useful in case a blanket reassessment is desired.

The New York Times Information Bank ("NYTIB") provides at the New York Times building both abstracts and full texts of articles published in that newspaper. From remote terminals, subscribers can search the compendium of abstracts for all articles which have been published in the New York Times and may request photocopies of the full articles whose abstracts satisfy the search criteria. The abstract searching can be full-text search, i.e., a search on the name "Harold Ickes" might result in a sheaf of abstracts, accompanying stories most of whose headlines say nothing about Ickes, but may refer to Roosevelt.

Full-text search capability is used in several states for purposes of law and legal decisions. In addition to struggling with the often inadequate index to such a corpus, an attorney can undertake a full-text search for statutes or cases which have some characteristics in common with his current concern.

The United States House of Representatives Bill Status Office handles over 1000 telephone inquiries each day concerning the status and content of legislation which has been introduced into the House.

All these are file-oriented systems, some of which may retrieve files according to the index system under which they were prepared; others, as we have seen, have a full-text search capability, such that a file can be retrieved in accordance with its *content* rather than heading.

Computer file systems are now in common use for text preparation and editing. A draft letter, report or publication is typed at a terminal connected with a computer (or sometimes at a stand-alone system). At any time, portions of the draft can be displayed, typed out locally or on a fast printer. The typist can enter corrections into the computer system (including global changes, e.g. to change the group of characters "seperate" every place it may occur into the group "separate"), can rearrange paragraphs, append additional files, and the like.

Use of files in intelligence work.—The work of intelligence agencies and their analysts is in large part the production of reports. There are routine periodic reports, reports in response to specific tasking on questions of concern to national leaders, reports which are initiated internally to the agency in response to some fact or complex of facts which seems to require attention at a higher level. In presenting any such material, the analyst needs to obtain as much other information about the subject (What is the significance of the appointment of an unexpected person as premier?) as is possible. There is a strong analogy to the NYTIB which should also serve to provide responsible reporters with other information on the subject of current interest (earlier, perhaps contradictory speeches of public officials, and the like).

Intelligence files may also have agents' reports, which are in the nature of fragmentary newspaper articles except that they are secret. Raw intelligence files may also contain the full text of foreign radio broadcasts as transcribed and circulated in printed form by the Foreign Broadcast Information Service (FBIS). If plaintext messages of a foreign military command are available, they will also be filed, and for efficient search and retrieval preferably in a computer store.

The use of computers in all these file applications—commercial, educational, and intelligence—is motivated by the same drive for efficiency, reliability and the capability to retrieve materials at places, times, and by persons other than those who have filed them. Computers at present are not normally used to store pictures or things, but indexes to such collections can as readily be placed in the computer as can any other kind of information. In contrast with a single physical file of paper documents, the computer store never suffers from the document's unavailability because it is on somebody else's desk. Multiple copies of a micro-image store can also satisfy the requirement for multiple simultaneous use, but cannot be updated or searched so readily as can a computer store.

Near-term future file technology: performance and cost.—In any case, it is not the purpose of this note to design a file system for the intelligence community, but rather to inquire as to certain aspects of privacy in regard to such files. The Privacy Act of 1974 is both the result and cause of increased interest in design of safeguards, which is at present the concern of an active subset of data-processing professionals and of a number of existing organizations,[5] including the Privacy Protection Study Commission, but a brief discussion of near-term future technology may be of help.

Obviously, concern regarding files and privacy is with the chain of information from collection through storage and retrieval. One worry is that some government organization by the expenditure of enough money, could have the capability to "know everything about everyone" at any time. Because there is no general public right of

[5] See for instance National Bureau of Standards Publications: FIPS PUB41—"Computer Security Guidelines for Implementing the Privacy Act of 1974" (SD Catalog Number C13.52:41) and "Executive Guide to Computer Security" (Available from the Institute for Computer Sciences and Technology, NBS, Washington, D.C. 20234).

access to the files of the intelligence agencies, it is of interest to know what these capabilities might amount to, as a guide to the introduction of safeguards.

In order to provide some intuitive feeling for the magnitudes involved, consider the storage of full page, double-spaced text. Such a page may have thirty lines of sixty-five letters or digits, or about 2,000 characters per page. Except as noted, it is assumed that a character requires one "byte" (8 bits) of storage, although by appropriate coding of text, one can store as many as three characters per byte.

Using a typical modern disk-pack magnetic storage device, storage of 300 million bytes can be obtained for a rental of about $1500 per month, or some $5 per month per million characters. Such a device can transfer about 1.2 million characters per second, so it would require 250 seconds to search its entire contents if the logical search device could operate at the storage data rate. Search is normally done by a query, looking for an exact match in the data stream as it is brought from the store. Examples of simple queries are: "theft of service" in the case of the legal corpus; "Chamberlain/Munich" in the case of the NYTIB (where the "/" simply means that both "Chamberlain" and "Munich" should be in the same document); "seperate" in the case of ordinary text processing where the properly spelled word "separate" is to be substituted. Such queries against a small data base are handled well by a general purpose computer. Indeed, large data bases also have some structure which can often be used to reduce by large factors the amount of data which actually has to be searched. But even if the data base has little structure, one could imagine streaming the entire data base past some modest special-purpose electronic device (a "match register") which may detect a match against the query and divert the matching document into a separate store, where it may be brought to the attention of the analyst. In large production, such a match-register might be bought for $100 in modern integrated-circuit technology. In any case, the cost of special-purpose match-registers would be small compared with the cost of the massive store and will henceforth be neglected here.

By such techniques, as many queries as are desired may be entered from terminals and simultanously matched against the entire data stream. If the data base is entirely in this type of storage (at a present cost of $5 per month per megabyte, or 50 cents per month per nominal file of 50 typed pages) any query can be answered within five minutes. Of course, a single query might lead to many other sequential queries before all the desired facts are at hand, but the time is measured in minutes, not months.

Given that most queries need not be answered in minutes, one can ask the cost of a slower system. There are now commercially available tape library products, of which a typical one can store 35 billion characters at a cost of about $18,000 per month (so 50 cents per million characters per month). This particular device can deliver data at a rate of 0.8 million characters per second, so that it would require some twelve hours for such a store to be searched entirely for as many queries as have been presented. The range of cost associated with such a system with current technology and twelve-hour response time thus

79-064 O - 76 - 37

goes from $10 million per month for a system capable of storing 50 pages on each of 200 million individuals (without encoding) to about $200,000 per month for a system storing the same amount of information on each of 10 million individuals, with the characters compacted into more efficient form for storage.

So much for the near term technology. It is being developed in this country and abroad entirely for commercial purposes. It serves highly important functions in allowing any organization—commerce, industry, government, and the professions—to manage information quickly and accurately.

Yet fresh in our memory is the use by the White House of the CIA to provide a "psychological profile" on Daniel Ellsberg. An ordinary file drawer would be adequate if one knew long in advance that information would be requested on this particular person. Given the unusual nature of the case and the non-existence of that particular file drawer, it would be technically possible to search all government files for documents which mentioned the name in question. This would bring to light, of course, income tax returns, military service history, all employees for whom social security tax had been paid in the past by the individual in question, names of relatives, etc. This material would not be found in *intelligence* files, but it could be found if the queries were made available to cooperating individuals with access to files in non-intelligence agencies like the IRS, Selective Service, and the like. Additional important information might be available by use of the NYTIB as a commercial subscriber.

Thus the problem in regard to those intelligence agencies with large files of raw data is to ensure that these files are used only in support of the authorized mission of the agency and are *not* exploited for purposes of improving prospects of incumbent officials in an election, of punishing those on an "enemies list," and the like. But it is no longer enough to proscribe the creation of specific files on U.S. citizens; it is now possible to recreate such a file from the central file in less than a day, or to answer questions from the central file without ever having a manila folder or file drawer labelled "John Smith." There must therefore be control over the queries asked of the file, of whom, and by whom. It is just as important to ensure that information given freely by individuals to non-intelligence agencies is not exploited for unauthorized purposes and is not accessible to unauthorized individuals.

The computer technology which makes possible rapid access to large masses of information also allows in principle for control of access to that information. Measures for preventing illegitimate use of government files could be proposed by the Executive, which can obtain help from equipment manufacturers, organizations experienced in computer use and analysis, and from the scientific societies. Such measures could be embodied in Executive Orders. Their adequacy and the need for legislation providing criminal and civil penalties should be the subject of Congressional hearings and research.

Safeguards which are being considered and partially implemented in non-intelligence files are the following:

1. There should be a limitation as to who can keep files on individuals. (But clearly the New York Times is allowed to put their own newspaper into computer-readable form. And

is it a file on an individual if the individual's name is only mentioned in a larger document?);

2. Individuals should be allowed access to their files (for repayment of the actual cost of search) and to receive the information in the file on them. (But if the file is very large, such access might be *made* very expensive. On the other hand, if the access were treated like an ordinary query in the example above, the cost might be quite reasonable.);

3. The individual should be allowed to write into the file in order to contest the facts or in order to present his own point of view;

4. There should be limitations on those who gain access to the file or who can receive information from the file;

5. Duplication of the file should be limited and unathorized access prevented;

6. There should be an indelible record of *who* has queried the file and *what* questions were asked, so that failure of access limitations will not go undetected.

Among the safeguards for any system should be adequate requirements for identification of terminals from which queries are being made, identification and authorization of the inviduals who query; a complete record of the queries (with terminal and individual identification), adequate security against transmitting large amounts of information and the like. The moment-by-moment execution of these controls on access is the task of the set of computer instructions known as the "operating system."[6] Although the design of an adequate operating system is a difficult task, the detailed specification of the controls is itself non-trivial and must be done with some understanding of what is technically feasible at present. Fundamental to the continued effectiveness of such safeguards is the maintenance of the integrity of the main program which controls the computer. Even in highly classified applications, there is no reason for this main operating program to be classified, and a source of strength should be public scrutiny of this operating system. Clearly, the introduction of access controls should not wait for the perfect operating system.

No matter what the safeguards, individuals might be able to gain access to some information for which they are not authorized. Adequate legislation, criminal penalties, and the enforcement of these laws should deter many who might otherwise try. Data security measures, such as encryption of the file itself, can help also.

What must be particularly guarded against is not so much the misuse of intelligence files but the misuse of information freely given or collected for authorized purposes and which is then turned to an improper use. Indeed, open analysis by all those concerned should lead to an understanding of the protection which may be provided.

---

[6] An introduction to the problem can be found in "The Protection of Information in Computer Systems," J. H. Saltzer and M. D. Schroeder, Proc. IEEE, Vol. 63, No. 9 (September 1975), pp. 1278–ff.

STATE OF THE ART OF ELECTRONIC SURVEILLANCE

Prepared by John S. VanDewerker, Ashby & Associates.

Ashby & Associates was formed in November 1968. In October 1971, its Systems Division was formed for the purpose of providing electronic security countermeasure products and technical services. After serving on a part-time basis with the Systems Division from 1971 to 1974, John S. VanDewerker became the general manager of that division in 1974. Mr. VanDewerker holds a BSEE from Washington State University, and completed graduate work in control systems at George Washington University. From 1967 to 1974, he was employed by the Central Intelligence Agency as a Program Evaluation Officer.

Commission Staff Note: The Commission's Request for a Proposal for a Study of the State of the Art of Electronic Surveillance advised contractors to include consideration of the following subjects and items:

1. Today's commercially available equipment for voice interception: kinds, basic characteristics, effectiveness, costs, and frequency of use. (Federally classified information is excluded.) Electronic components and their potential for use in assembling illegal devices should be explored.

2. Countermeasures: Examples, capability, cost, effectiveness. What is envisioned is a rather brief commentary on countermeasure equipment, its use, and effectiveness with respect to the kinds of commercially available equipment discussed in item 1, above.

3. Other kinds of communications which are subject to interception: transmission of data from computer to computer, pen registers, telephone decoders, etc.

4. Aids to physical surveillance: video cameras and "bumper beepers," etc.

5. Today's technology and its impact on tomorrow's threat to the invasion of privacy: the practical application of science to electronic surveillance in the forseeable future, to include consideration of such matters as miniaturization, integrated circuits, laser, radar, infra red, X-rays, voice prints, optical fiber (integrated optics), and higher frequency transmission.

CONTENTS

Acknowledgements
Abstract
Review of Terminology
Introduction
Objective
Methodology
Summary of Findings
Conclusions
Recommendations
Equipment Characteristics and Capabilities
1.0 Audio Eavesdropping
1.1 Telephone Systems
1.1.1 Telephone Wiretapping
1.1.1.1 Wire Systems
1.1.1.2 Radio Systems
1.1.1.3 Accessories
1.1.2 Telephone Room Eavesdropping
1.1.2.1 Infinity Transmitters or Harmonica Bugs
1.1.2.2. Listen-Backs and Keep-Alives
1.1.2.3. On-Line Microphones
1.1.2.4 Telephone Modifications
1.1.2.5 Radio Frequency Flooding
1.1.3 Summary of Telephone Device Characteristics
1.2 Microphone Systems
1.2.1 Types of Microphones
1.2.1.1 Carbon Microphones
1.2.1.2 Magnetic Microphones
1.2.1.3 Speakers
1.2.1.4 Condenser Microphones
1.2.1.5 Electret Microphones
1.2.2 Special Purpose Microphones
1.2.2.1 Contact, Spike and Pneumatic Microphones
1.2.2.2 Parabolic and Shotgun Microphones
1.2.3 Microphone Devices Summary
1.3 Radio Eavesdropping Devices
1.3.1 Inexpensive Devices
1.3.1.1 Wireless Microphone Transmitters
1.3.1.2 Fabrications
1.3.2 Drop Transmitters
1.3.2.1 Miniature Devices
1.3.2.2 Agent Transmitters
1.3.2.3 Concealment Packages
1.3.2.4 Modulation Techniques
1.3.3 Carrier Current Devices
1.3.4 Microwave Devices
1.3.5 Passive Reflectors
1.3.6 Remote Switch Receivers
1.4 Tape Recording Systems
1.4.1 Briefcase Concealment Packages
1.4.2 Miniature Devices
1.5 Optical Directional Systems
1.6 Summary of Eavesdropping Device Characteristics
2.0 Audio Security Countermeasures
2.1 Telephone Systems
2.1.1 Telephone Taps
2.1.1.1 Wire Systems
2.1.1.2 Radio Systems
2.1.2 Telephone Room Eavesdropping Devices
2.1.2.1 Infinity Transmitters, Listen-Backs and Keep-Alives
2.1.2.2 On-Line Microphones
2.1.2.3. Telephone modification
2.2 Radio Eavesdropping Device Detection
2.2.1 Field Strength Measurement
2.2.2 Countermeasures Receivers
2.2.3 Spectrum Analysis
2.2.4 Other Inspection Equipment
2.3 General Purpose Audio Surveillance Protection Systems
2.3.1 Acoustic Protection
2.3.2 Radio Frequency Protection Systems
2.4 Audio Countermeasures Services
2.5 Summary of Audio Countermeasures Devices
3.0 Intercept of Non-Audio Information
3.1 Bulk Data Communications Systems
3.2 Computer Systems
3.3 Optical Processing Systems
4.0 Electronic Aids to Physical Surveillance
4.1 Night Viewing Systems
4.1.1 Passive Imaging Systems
4.1.2 Active Imaging Systems
4.1.3 Electro-Optical Solid State Imaging
4.2 Tracking Systems
4.2.1 Radio Direction Finding
4.2.2 Time Difference of Arrival Systems
4.2.3 Coordinate Systems
5.0 Projection of Surveillance Technology
5.1 Audio Systems
5.1.1 Telephone Systems
5.2.1 Radio Transmitters
5.1.3 Microphone Systems
5.1.4 Recording Systems
5.2 Physical Surveillance
Glossary
General Bibliography

LIST OF ILLUSTRATIONS

Figure 1—Frequency Spectrum Chart 145
Figure 2—Magnetic Microphone 148
Figure 3—Magnetic Earphone 148
Figure 4—Inductive Sensing 149
Figure 5—Telephone System Eavesdropping 159
Figure 6—Radio Tap Transmitters 162
Figure 7—Various Microphone Types and Methods of Covert Installation 169
Figure 8—Magnetic Speakers Used as Surveillance Microphones 170
Figure 9—Carrier Current Transmitter 176
Figure 10—Passive Cavity Transmitter 178
Figure 11—Optical Audio Eavesdropping 181
Figure 12—Field Strength Meter "Bug" Detectors 189
Figure 13—FM Broadcast Band Spectrum 191
Figure 14—Radio Spectrum Display 194
Figure 15—Cost Versus Frequency Coverage of Radio Detection Devices 195
Figure 16—Radio Devices Transmitting Power vs. Effective Range 196

LIST OF TABLES

Table I—Telephone Devices Summary 167
Table II—Microphone Devices Summary 172
Table III—Eavesdropping Devices Summary 183
Table IV—Audio Countermeasures Equipment 200

ACKNOWLEDGEMENTS

The authors wish to express appreciation to the following individuals for their assistance, recommendations, and contributions made during the course of this study and their worthwhile opinions which were frequently solicited:

Mrs. Sybil S. Barefoot
Mr. Glenn A. Burklund
Mr. Charles E. Gaskin.

ABSTRACT

The Science of Electronic Surveillance

This document presents the results of an extensive data gathering and analysis effort, organized and completed over a seven month period, and addresses each of the following five areas:

1.0—Eavesdropping Equipment—This Section includes a review of telephone eavesdropping devices, radio transmitters, passive and active listening devices, audio system accessories, and sophisticated eavesdropping techniques.

2.0—Countermeasures Equipment—This Section discusses counter-surveillance radio receivers, telephone analysis equipment, electronic aids to physical inspection, and protection devices such as acoustic rooms, disconnect devices, filters, and various radio jammers.

3.0—Penetration of Other Information Handling Systems—This Section addresses computer security and eavesdropping on information processing machines.

4.0—Electronic Aids to Physical Surveillance—This Section reviews night viewing devices and systems, and various tracking devices such as beacons and radio navigation systems.

5.0—Systems of the Future—This Section projects the development of surveillance technologies into systems which may become available in the foreseeable future. These include various devices for signal and voice processing, radio modulation and transmission, electo-optical imaging, and information recording.

As an aid to the non-technical reader, a brief tutorial defines basic terminology and scientific principles that allow understanding of eavesdropping devices and practices. This electronics primer is enhanced by a glossary of terms to guide the reader through the text.

As a summary of the extensive presentation regarding equipment characteristics and capabilities, a series of findings ascertained during this study are presented. Conclusions drawn from these numerous findings are presented as are several recommendations that effect a purpose for the completion and documentation of this work.

REVIEW OF TERMINOLOGY

A comprehensive discussion of the state of the art in any technology requires that the reader be familiar with the basic concepts of that technology so that full appreciation of the information presented is possible. So it is with this report wherein, not only an understanding of the basic electronic and physical concepts is required, but also an understanding of the practice of audio surveillance is necessary. Uncertainty with these concepts can cause ambiguities in the reader's mind, which reduce appreciation for the characteristics and operational capability of specific electronic surveillance tools.

It is the intent of this introductory section to familiarize the reader with the technical concepts that are used repeatedly in the text and bring a level of understanding sufficient for obtaining full benefit from the discussion. This introduction, when reviewed in conjunction with the Glossary, should provide a basic understanding of the technical concepts of: frequency, electrical energy, magnetism, and modulation, and their place in the world of electronic surveillance.

Frequency

Frequency is one of many terms used to describe a characteristic common to microphones, radio transmitters, surveillance receivers and even laser light beams. It refers to the number of times a cyclical motion such as a vibration is repeated in a specific time interval. If the time interval is equal to one second, the frequency is the total number of times per second the repetitive incident occurs and is referred to as Hertz and is abbreviated Hz. This term is named in honor of the German physicist Heinrich Rudolf Hertz, 1857-94, who discovered radio waves. For example, a room fan which revolves ten times in one second has a frequency of 10 Hz; human speech generated by the vibrating vocal cords consists of audible sounds with frequencies generally in the range of 90 Hz to above 7,000 Hz. A range of frequencies is referred to as a spectrum or frequency band. In this case, human speech has a spectrum on the order of 90 Hz to above 7,000 Hz.

The concept of frequency is consistent regardless of the particular surveillance device being described. As frequencies increase they occur higher in the total spectrum of frequencies; above those of human speech are radio broadcasts, television and light. The complete frequency spectrum is illustrated in Figure 1.

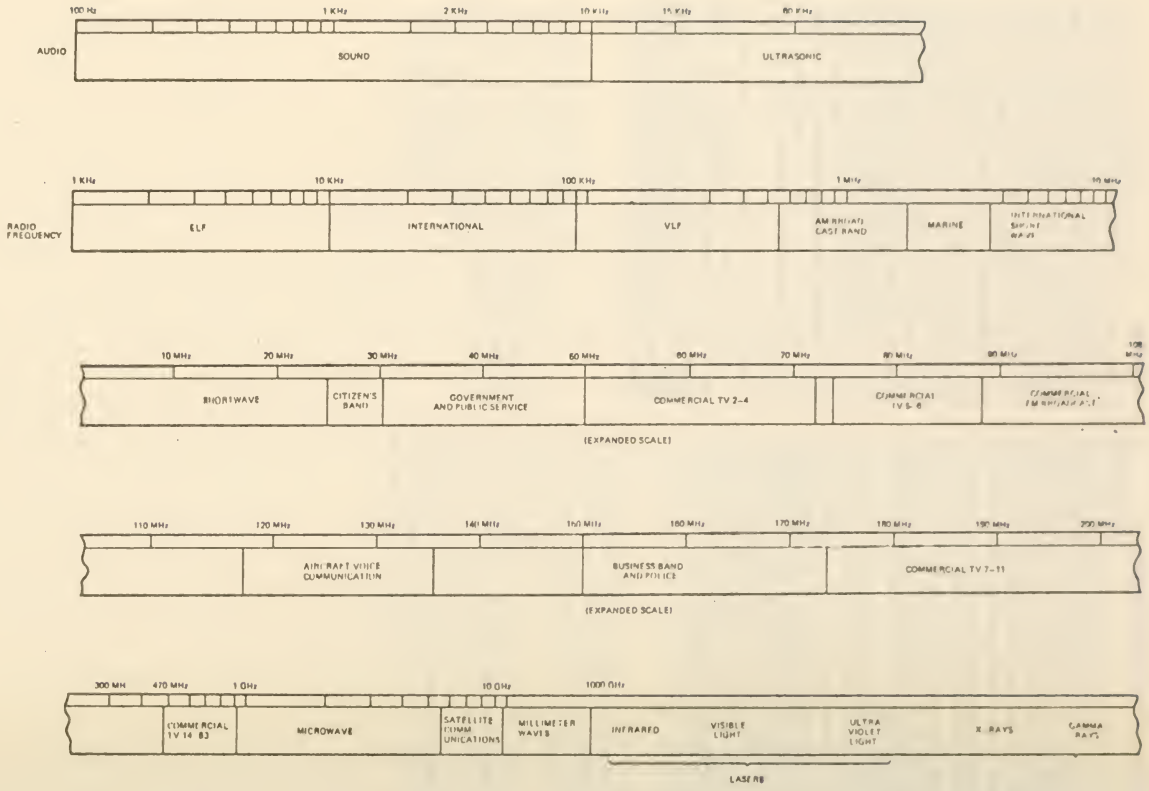


FIGURE I. FREQUENCY SPECTRUM CHART

In the radio frequency range of 550 thousand to 1,600 thousand Hz (Kilo Hertz [KHz] for thousands of cycles per second) is the commercial AM radio broadcast portion of the spectrum. At 88 MHz to 108 MHz (one thousand KHz is one million cycles per second and is known as Mega Hertz [MHz]) is the standard FM commercial broadcast band. The terms Kilo (thousands) Hz and Mega (millions) Hz refer to the number of times per second the radio energy is varying and these abbreviated terms are much easier to use in discussions of electrical characteristics than thousands and millions of cycles. Above the commercial radio broadcast frequencies are frequency regions known as Very High Frequency (VHF) and Ultra High Frequency (UHF). Most commercial radio eavesdropping devices operate at frequencies in these regions. Figure 1 also illustrates the many channels or radio frequencies allocated by the Federal Communications Commission (FCC) for a specific use. For example, aircraft voice communications use the frequency spectrum between 118 MHz and 138 MHz; police use frequencies between 150 MHz and 160 MHz.

Frequency specification is critical to the description of eavesdropping radio transmitters and receivers because it immediately identifies where in the spectrum the transmitter emits its signal and likewise where the receiver must be tuned to receive it. Because of this allocation of frequencies and the need to have a companion receiver with each transmitter, many eavesdropping transmitters operate in or near the commercial broadcast portions of the spectrum because easily modified, inexpensive portable radio receivers can be used to receive these signals. In the eavesdropping business operating frequencies are carefully selected to prevent casual or accidental detection, but the price paid for increased freedom from detection may be high. In general, as transmission frequency increases so does the cost of both the transmitter and receiver.

Other performance characteristics controlled by transmission frequency are the effective transmission range, susceptibility to static or other electrical noises, and ability to pass through or around large physical objects such as hills or buildings. These latter characteristics become more acute as frequency increases to the point where the radio signal will travel only in a straight line and pass very poorly through or around solid objects.

Understanding the concepts of frequency and spectrum is important to understanding the advantages or limitations of a specific surveillance device. In many cases frequency may be the only technical difference between devices and be the major determining characteristic which controls cost, performance, and capability.

Energy

Energy is a term used to describe an ability to perform work; the greater the energy, the greater is this ability to work. Energy identifies one aspect of the capability of a material or device, such as the energy contained in a gallon of gasoline, the sun's solar energy which can heat a home, or the stored energy in a lake behind a dam which can be converted to electrical energy and routed over wires to a consumer. In this report, electrical energy is discussed from several viewpoints including electrical voltage, electrical current, and electrical resistance, since each affects the performance of an eavesdropping device.

To develop an appreciation for these electrical terms, consider the analogy of a water pipe and spigot in a conventional household plumbing system. In this comparison, the water pressure is equivalent to electrical voltage and water flow equivalent to electrical current. If the spigot is closed, the pressure behind the spigot exists within the pipe; if the spigot is opened, water will flow out depending on the size of the opening and the amount of pressure. In this case the flow of water is controlled by the pressure in the pipe and the size of the opening which offers some resistance to the flow. In an electrical equivalent, when a power source such as a battery exerts a voltage pressure on an electronic device, the amount of current which flows depends on the resistance offered by the device and the capacity of the battery.

In the normal household, the voltage pressure is 110 to 120 volts and the electrical flow of current is limited by a fuse in the fuse-box or circuit breaker to about 20 amperes. Volts are the measurement units for voltage and amperes are the measurement units for current. The simple "D" size flashlight battery has a voltage of only 1.5 volts and a current flow cabability of approximately one-half ampere. It is important to note here that the physical size of a battery does not change the voltage available, only its capacity to supply a large flow of current. These two electrical characteristics of voltage and current, when multiplied, result in the total power consumed by an electronic device and is expressed in watts. For example, in the case of the flashlight battery, if 1.5 volts is multiplied by 0.5 amperes the resulting power is 0.75 watts.

All batteries supply direct current meaning that neither the current nor voltage varies regularly with time, but household current does vary at a fixed frequency of 60 Hz. In the home a 150 watt lightbulb operating from a 110 to 120 volt AC

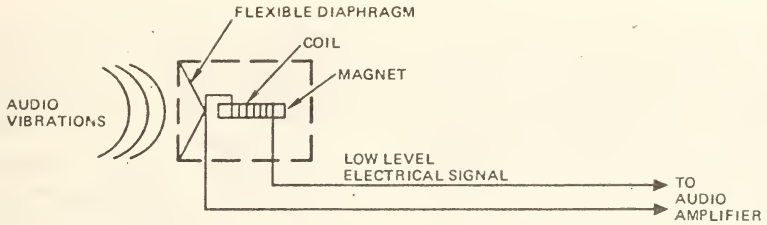
(alternating current) circuit would draw approximately 1.4 amperes of electrical current. A lightbulb with a higher power rating, such as 500 watts, would consume more current but illuminate a larger area. The concept of power in a surveillance device connotes that greater power provides greater operating range at the same frequency. Unlike lightbulbs, most eavesdropping devices consume and radiate only 1/100th to 1/10,000th the power available from household electrical wiring. For these reasons, the terms milliwatt (mw), meaning 1-1000th of a watt, millivolt (mv), meaning 1-1000th of a volt, and a milliampere (ma), meaning 1-1000th of an ampere, were formed to permit easy expression of these smaller units of electrical characteristics.

Throughout the technical discussion of this report, the term milliwatt is occasionally used to specify the power of a surveillance device. It is the basic electrical characteristic which can usually be related to the effective operating range of a surveillance transmitter. In the electronic surveillance area, amounts of power are generally small and the usual clandestine transmitter is rated at ten to twenty milliwatts, which, depending on frequency and other physical factors, may have a range of one to six city blocks. Higher powered body transmitters may produce 100 milliwatts to 1 watt and beacon tracking transmitters 1 to 2 watts. The ranges associated with the higher powered devices are usually in excess of 6 blocks and could be several miles under favorable conditions.

The effect of power consumption on battery life is of great importance. A device consuming ten milliwatts which operates for ten hours from one battery of a specific size, may operate one-half as long from a battery of one-half the capacity and conversely, doubling the battery capacity may double the transmitter operating life. Increasing the voltage does tend to increase the power output of the device and thus increases the effective operating range. This latter technique is common practice for a user of the so-called wireless microphone where a single battery is replaced by two batteries in series which increases the effective range of this transmitter.

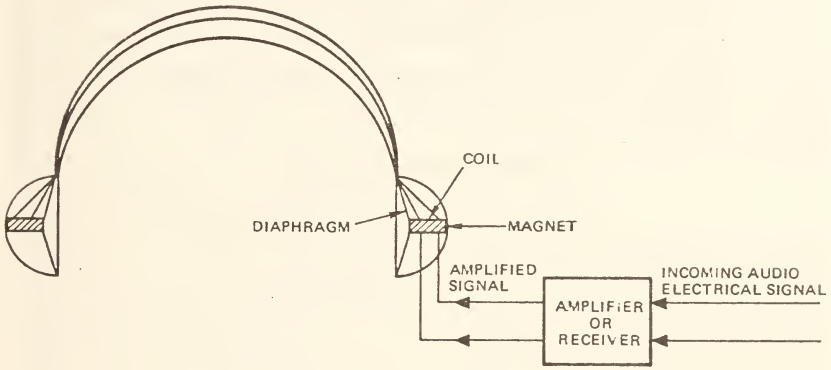
Magnetism

Magnetism is recognized in its steady, unvarying state as that force which is present in a simple permanent magnet. If, however, the physical position of this force is changed while in the vicinity of a length of wire, an electrical current will flow through this wire. By exploiting this electrical phenomena, several beneficial things can be made to happen including the generation of electrical power and the conversion of audio sound into electrical signals. Any changing or moving magnetic field will induce a current flow in a piece of wire and conversely, any current flowing through a piece of wire will create a proportional magnetic field. This reciprocal relationship between electrical current and magnetism is a key factor in the technical performance of several basic eavesdropping devices. One device commonly used in conducting electronic surveillance is the magnetic microphone which converts audio sound vibrations into electrical signals by vibrating a coil of fine wires in a magnetic field as shown in Figure 2. Another is the sensing of a magnetic field which surrounds the telephone instrument and transmission wires with a small coil of wire or induction coil as shown in Figure 4. Here, the changing magnetic field induces or generates a proportional electrical signal in the coil. Even the eavesdropper's earphones, Figure 3, behave in this same predictable manner; the electrical signal flowing through a coil of wire generates a magnetic field which moves a thin metal plate or diaphragm at an audio frequency rate which in turn vibrates the air creating sound that can be heard by the human ear.



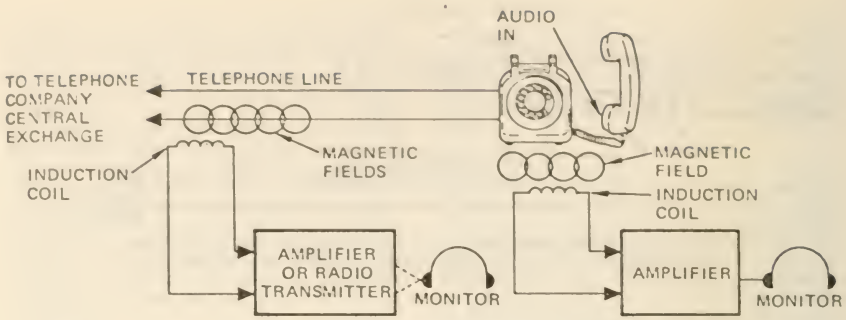
ELECTRICAL SIGNAL GENERATED BY COIL MOVEMENT AROUND MAGNET IS PROPORTIONAL TO AUDIO VIBRATIONS PRESENT AT DIAPHRAGM

FIGURE 2. MAGNETIC MICROPHONE



AMPLIFIED ELECTRICAL SIGNAL APPLIED TO COIL CREATES DIAPHRAGM MOVEMENT. DIAPHRAGM MOVEMENT REPRODUCES INCOMING ELECTRICAL SIGNAL AS AN AUDIO SIGNAL

FIGURE 3. MAGNETIC EARPHONE



MAGNETIC FIELD SURROUNDING TELEPHONE WIRE AND INSTRUMENT IS PROPORTIONAL TO THE AUDIO SIGNAL

INDUCTION COIL TRANSFORMS MAGNETIC FIELD VARIATIONS TO AN ELECTRICAL SIGNAL

LOW LEVEL ELECTRICAL SIGNALS ARE AMPLIFIED FOR AUDIO MONITORING OR RADIO TRANSMISSION

FIGURE 4. INDUCTIVE SENSING

In the context of this report, measurement of magnetism is not necessary because the basic understanding of this relationship between electrical signals and magnetic or inductive forces is all that is required to appreciate the significance of many surveillance techniques.

Modulation

The term "modulation" means to momentarily change or vary with time some normally unvarying and continuous process. These brief variations correspond directly to some desired message. In a crude sense this would include turning on and off a light switch in a series of dots and dashes to modulate the intensity or amplitude of light energy from a lamp. Furthermore, if groups of these dots and dashes correspond to alphabetic letters, as in Morse Code, a message is contained in this modulated light. This modulation is known as digital, pulse, or on-off keying and is similar to that used by teletypewriters or computer terminals. If this light switch were replaced by a dimmer type control, the lamp could be turned up and down to vary the light intensity without completely turning it on and off. If this intensity is varied rapidly and continuously, corresponding to the frequencies contained in human speech, then the amplitude of the light is being modulated in an analogue fashion rather than a digital or pulse mode.

In radio communications the amplitude of a single radio frequency, perhaps 100 MHz, could be switched on and off or varied continuously in the same manner as the light and likewise carry the same message. In this case the radio signal could carry the message over a considerable distance. This is Amplitude Modulation (AM), one of the earliest forms of modulation and is still used today in the commercial AM broadcast band.

Since the process of modulation means momentarily varying any stable characteristic of a signal, such as the amplitude or intensity of the signal, other continuous characteristics may also be varied or modulated. Again, consider the single frequency radio signal operating continuously at 100 MHz. Rather than momentarily turning the signal off and on and thereby change its amplitude, slightly change the frequency. Now, rather than operating at exactly 100 MHz, the radio signal frequency might be varied at an audio rate about the central frequency of 100 MHz. If this process is repeated corresponding to a desired message, then the radio signal is being frequency modulated (FM) rather than amplitude modulated (AM) as described in the earlier example of the on/off light switching or intensity variation.

These modulations are known conventionally as FM and AM and each is one specification of surveillance device performance, since the reception or detection of these devices requires specific knowledge of the modulation being used. The eavesdropper, by controlling the type of modulation used in a clandestine device, may incorporate additional privacy and freedom from discovery since the choice of modulations are numerous. In some cases a single radio frequency could be modulated a number of times to prevent accidental detection. In a sense, knowing the modulation technique chosen for use in an electronic surveillance device is a key factor to receiving the radio signal and being able to decode, that is, understand the message.

When a single radio frequency carrier is modulated by an audio signal that contains frequencies of 3000 Hz, the single carrier frequency will vary over a limited excursion about this single frequency. This excursion is known as the "bandwidth" of the radio signal. If a radio receiver is tuned to the radio carrier frequency, it must have at least the same bandwidth capability to receive and process the 3000 Hz audio signal. The concept of bandwidth is important in specifying the performance and capability of a receiver or radio detection device, for if the receiver does not have the necessary bandwidth, it will not receive and effectively demodulate the signal.

INTRODUCTION

The reasonable expectation of privacy is an individual's right guaranteed within the broad legal framework of our open society. This guarantee, however, has become increasingly difficult to ensure because of the advent of surreptitious electronic devices which are now found throughout this country. The public was basically unprotected from technically inspired invasion of privacy until 1968 when the Omnibus Crime Control and Safe Streets Act became law. Title III of that Act was designed to protect each American's privacy from intrusion by the mechanisms of electronic surveillance, except under certain limited and specifically prescribed circumstances recognized by the U.S. Supreme Court as being constitutionally permissible.

This legislative effort to control surveillance has been tested for over six years. Rapid advances in electronic technology have opened new avenues for surveillance techniques; some are extremely complex, such as the "laser window pickoff", and some are deceivingly simple, such as the "telephone compromise". For the most part, the technology application is easily within the capabilities of the elec-

tronic technician and hobbyist. To this readily evident environment may be added the conjunctive conditions of improved technical communications, cross fertilization of ideas by electronic engineers which is enhanced by job mobility, and increased availability and reduced costs of components which arise with the enhanced productivity of the blossoming electronics industry. Congress exercised remarkable foresight in mandating by statute that a National Commission would review the first six years of experience under this law and would report to the President and the Congress whether any changes should be made.

OBJECTIVE

The purpose for conducting this study is to assist the National Wiretap Commission in defining the characteristics, effectiveness, use, and cost of electronic eavesdropping devices and other technically facilitated invasions of privacy by establishing the current state of the art in surveillance technologies. It is intended to be a thorough review and summary that is descriptive of devices used by public law enforcement organizations and by the domestic sector in private and industrial surveillance activities. This overview is a summary of equipment characteristics including voice communications gathering effectiveness, frequency of use, and device costs. Also included within the scope of this document is a review of other electronic aids for information gathering and individual surveillance. These include computer data intercept techniques, vehicle and cargo tracking systems, and low light level imagery or night viewing visual aids. To provide the Commission and the public with a realistic perspective of electronic privacy invasion, the report also presents a critical review of those defensive electronic countermeasures devices and services which are available for those who seriously believe that their privacy is being threatened.

Since the objective of this Commission is to review the effectiveness of legislation enacted in 1968 and offer constructive criticism in the form of recommendations for modifying legislation, a liberal amount of forward thinking is necessary. Therefore, the reasonable projection of futuristic electronic threats is of importance for an effective definition of recommendations that are anticipatory of tomorrow's needs. This projection is one principal goal of this study.

METHODOLOGY

Information for this report was gathered and substantiated by completing four basic tasks. These included:

a. Interviews with over 18 select members of the law enforcement, federal, and industrial communities familiar with the surveillance technologies;
b. Survey of 120 law enforcement organizations determining surveillance device type, inventory, frequency and practices of use;
c. Collection and review of over 200 equipment catalogues in the audio, visual, and physical surveillance fields; and
d. Identification and assembly of over 180 published journal articles, books, advertisements and government reports.

Data gathered from these sources were subject to critical review and analysis to determine their relevance to this study and to insure its technical integrity.

SUMMARY OF FINDINGS

This summary presents the principal findings determined as a result of this study and subsequent analysis. Findings are grouped according to subject areas. The numerous devices that are distributed into these five areas are the focal point of examination in this study, and are discussed in detail in another section in this report.

Audio Eavesdropping

Findings in this area are divided among: telephone system surveillance, microphones, radio transmitters, optical transmitters and recording devices.

Telephone System Surveillance. Various audio eavesdropping devices use or exploit the telephone system in two distinct ways: those which intercept actual telephone conversations; and those which use parts of the system to facilitate room eavesdropping. Use of some devices requires access to the target area or instrument prior to eavesdropping, while other techniques do not necessitate entry to the premises to implement the eavesdropping.

The interception of normal telephone conversations, or wiretapping, is conducted either by connecting a listening device directly to the lines (hardwire tap) to by attachment of a radio transmitter. All parts required to complete a hardwire tap are available to the private sector without restriction because, individually, each component is not identifiable as an audio eavesdropping device. The devices used for successful radio tapping of the telephone, however, are not readily available because of their apparent eavesdropping nature and are more costly and usually less reliable in use than those required for hardwire tapping. For these

reasons, and for its superior security, the hardwire tap is the more frequently used technique among law enforcement organizations.

Portions of the normal telephone system may be manipulated or modified and made to serve as part of the audio eavesdropping system. One device that uses part of the telephone system, the infinity transmitter, performs well as a room bug and is offered for sale to the public as a burglar alarm.

Room eavesdropping is also possible with a modified telephone instrument, where the handset serves as the microphone, and the modified instrument uses additional electronic parts which are inexpensive and readily available in most radio-TV and electronic retail stores. The use of this latter technique is limited, however, because of the technical skill and expertise required to modify the telephone instrument.

Microphones. Recent developments in microphone technology, due in part to growth of the commercial tape recorder and hearing aid market, have resulted in abundant supply of very small microphones. Singularly, microphones do not constitute an electronic eavesdropping threat because additional components are required to make a complete surveillance device. The procedure of room eavesdropping by use of a small microphone and wire system, although most reliable and virtually undetectable, remains unattractive to eavesdroppers because of the difficult installation problem and the technical expertise needed to assure proper operation.

Radio Transmitters. Radio transmitters used for eavesdropping are generally restricted to those devices small enough for easy concealment. Three groups of transmitters were found to satisfy this criterion, each identifiable by relative differences in cost, sophistication, and availability.

The least costly, most available, and widely used devices in the private sector are identified as baby monitors or wireless microphones in mail order or magazine advertisements. These devices were found to be in most frequent use, since they require little, if any, modification, are difficult to trace to the user of the device, are inexpensive, and require an inexpensive portable radio normally used for commercial broadcast reception. Their principal limitations are short range, poor reliability, and high probability of accidental detection, since they usually operate directly in or near the commercial FM broadcast radio frequency band.

The second category of transmitters are those inexpensive devices not readily identifiable as surveillance devices and which require modification by the eavesdropper for conversion to a surveillance device. Within this group are inexpensive walkie-talkies, or two-way radios, used in citizen band and amateur radio equipment.

The sophisticated group of transmitters includes those used by law enforcement. These tend to be more effective, smaller, and more secure for surveillance applications. These are frequently offered for sale preconcealed in various household fixtures such as ashtrays, picture frames and lamps.

Optical Systems. Audio eavesdropping systems exist which operate by using either visible or nonvisible light beam transmissions to carry audio information. These systems function either as a communications link between a planted surveillance device and the listening post or as an illuminating beam of light energy that retrieves audio vibrations from a target area by bouncing the light from a vibrating, reflective surface such as a window.

The use of light beams for point-to-point communications is fairly common in industry. Equipment, both transmitters and receivers, although expensive, are commercially available. A very attractive feature of an optical eavesdropping link is the low probability of detection during use. This feature, however, is offset by difficult installation and operational problems and this technique is relatively unattractive for the eavesdropper.

The use of laser beams to retrieve audio from vibrating window panes, although highly publicized, was not found to exist outside the experimental laboratory. This technology offers no substantive threat at the present time because of the high cost of special equipment, restrictive physical considerations, and skill required for successful operation.

Recording Devices. A number of recording systems were identified which allow operating times of up to eight hours and a few with recording durations of twenty-four hours without the need to change recording tape. Each was a component of a recording system designed for use by the police, telephone companies, airlines, or the entertainment industry. They were not found to be attractive as a part of a surreptitious audio eavesdropping system, mainly because of size and cost.

Standard cassette recorders were frequently found coupled with voice actuation switching devices designed to extend their operating time and provide unmanned operation. Typically, these systems were prepackaged in standard briefcases and controlled by concealed switches. The microphone is usually hidden behind the briefcase clasp, lock, or hinge and installed to ensure good performance while the briefcase is closed. These nominally priced systems were not found to be readily available to the private sector because of their obvious audio eavesdropping capabilities. Several complete briefcase units were found which

contained not only voice actuated recorders but also radio receivers that permit automatic recording of signals received from a remote, companion radio transmitter

Recording system miniaturization technology has provided the audio surveillance practitioner with small units having operating times of approximately one hour. One, the size of a cigarette lighter, operates for several hours but is quite expensive and available only through European outlets. Slightly larger but less costly devices have become quite popular for short term recordings and are used in a consensual environment.

Countermeasures

Audio countermeasures is the term used to describe the encompassing practice of detecting audio eavesdropping devices or protection from the effects of these devices. It requires both a skilled technician and sophisticated electronic equipment and is commonly termed "debugging".

Findings fall into four categories: telephone systems, microphones, radio transmitters, and service organizations.

Telephone Systems. No countermeasures equipment was found which could conclusively determine the existence of a properly installed wiretap. Furthermore, it was determined that only close visual inspection of the entire telephone line could resolve this question.

Several companies offer electronic telephone instrument analysis equipment which, if properly operated, could determine the existence of a tone activated infinity transmitter as well as numerous types of telephone instrument modifications.

A limited number of suppliers were found which offer systems designed to protect the individual from eavesdropping resulting from telephone modifications. These equipments include switching devices to isolate the unused telephone from the external telephone wires and jamming devices that inject noise into the instrument or telephone lines to make them unuseable for eavesdropping.

Microphone and Wire Systems. No countermeasures equipments were found that reliably locate microphones. Metal detectors may locate a microphone, if it is installed in an area where no other metal objects exist and the detector passes in close proximity to the microphone.

Radio Transmitters. Radio transmitters used for surveillance can be located in many ways with equipment offered by many manufacturers. These detection units were found to exist in three generic categories: radio signal energy measuring devices (field strength meters or "sniffers"), radio frequency analyzers (spectrum analyzers), and countermeasures radio receivers or combinations of these equipments. If the eavesdropping transmitter is active and transmitting a radio signal, any of the aforementioned detectors may determine its presence. In general, for any given situation the performance of the radio signal energy measurement device is inferior to both the analyzer and countermeasures receiver. The latter two are frequently used together to provide the operator an increased analytical capability.

Service Organizations. Few commercial organizations were found that were able to demonstrate extensive competence in performing the services of audio countermeasures device design, facilities technical inspection, protection from surveillance invasions, or consulting services. Six firms were found that appeared to have sufficient electronic countermeasures equipment and professionally trained, experienced personnel to perform this service. Unfortunately, in the private sector it is difficult to identify competent countermeasures organizations. While it is legal to advertise countermeasures services, the media is reluctant, by policy, to accept such advertising because of fears regarding misrepresentations by the advertiser. Further, no licensing procedures or standards exist by which service organizations are evaluated and by which evaluations are made known to the public.

Interception of Non-Audio Information

Intercepting non-audio information means intercepting those communications which are not human speech. Specifically, this includes teletype and bulk or multi-channel data communication transmissions, computer data, and information processing machine emanations. These types of interceptions are not addressed in Title III of the Omnibus Crime and Safe Streets Act of 1968, which defines an intercept as the "aural" acquisition of a wire or oral communication.

Bulk Data Communication Links. Radio receiving equipment was found to exist and is publicly available that permits the interception of communications channels. After signal reception by the eavesdropper, however, signal processing is required to reconstruct the audio information. This technical imposition removes this practice from most conventional eavesdropper's capability. This information gathering activity was found to be of interest principally to federal organizations and some large corporations.

Computer Systems. This area was found to be by far the most active in non-audio eavesdropping. Interception and manipulation of data occurs between a time-shared computer subscriber remote terminal (such as at banks, credit bureaus, or secu-

rities brokers) and the central computer. Signal reception can be implemented through the use of standard audio eavesdropping devices and is difficult to trace. Interpretation and control of the digital data signals requires the use of a modestly expensive computer keyboard terminal and in some cases a mini-computer. The technical skills required are moderate but the rewards for the eavesdropper may be considerable, and therefore, quite attractive to the skilled, professional criminal. Awareness of this interception activity has caused industry to increase computer security, a difficult task in view of the diversified talents of private sector computer eavesdroppers.

Electronic Aids to Physical Surveillance

It was found that extensive electronic assistance is available to law enforcement and security organizations for night viewing and vehicle or cargo tracking. The market for these aids was found to be much greater than for audio eavesdropping devices. All devices available are apparently legal as none of these items are considered to be eavesdropping devices. The devices only assist human senses and have an established position in the physical security field. A brief statement of findings is made below.

Visual Systems. Several manufacturers offer small, hand-held, light amplifying or illuminating devices which permit the detection of a human being at one thousand feet and identification at approximately one-fifth that distance under very low light level conditions. All systems were found to vary greatly in size, cost, capability, and application, ranging from direct viewing pistol grip devices to night observation devices with large lens extensions. All devices and systems were found to be expensive and some systems afford photographic or video capability.

Tracking Systems. Most vehicle and cargo tracking systems found to be used by law enforcement agencies consist of a beacon transmitting device and a companion receiving device to detect these signals. Tracking systems vary in quality depending upon the amount of radio signal processing done to determine range and direction of the beacon from the receiver. Generally, most systems provide a left-right meter indication of direction and a relative range estimate to the operator. Each system was found to be moderately expensive. Use of tracking systems varies greatly among organizations because of the level of operator skill required for successful operation. Most systems were capable of operation from both aircraft and automobiles with the superior performance being experienced with the former.

Several newer technologies were identified which allow simultaneous tracking of many vehicles from a single control station. These systems are not uniquely applicable to covert law enforcement tracking operations; however, due to the high capital investment, size, and complexity, such systems were found to be intended for civil use in traffic and mass transit systems management.

Systems of the Future

There is minimal value in assessing the current status of electronic eavedropping systems for the purpose of conceiving legislation intended to be effective in the future. A projection of these eavesdropping technologies was made in the areas of communications systems, microphones, and recorders, since each is critical to future capabilities of electronic privacy intrusion devices. Future technology, in general, is developing from the advancement of commercial industries.

Communications. New developments in the telecommunications industry were found and others are expected that will make surveillance more difficult for the electronic eavesdropper. This is primarily due to anticipated telephone and visual system developments, including optical fibers which carry light energy, and special high frequency radio signals which are conducted inside buried, metal pipes. These developments are being stimulated by the need for larger capacity communications systems and not by improved security needs. Because of the technical complexities involved, it can be surmised that eavesdroppers of tomorrow will be faced with a very complex problem; however, judging from past performance and the technical ingenuity displayed by the eavesdropper, it may be expected that any communications system of the future could be compromised.

Radio Transmitters and Receivers. The current physical size of radio transmitters and receivers used in electronic surveillance will undoubtedly diminish, but this may be of limited benefit if battery technology does not progress at a similar rate. If not, the size of an easily concealable listening device will be limited by its battery power supply.

It has been found that an emerging technology may partially solve this size problem. New microcomputer processor techniques of the type provided in pocket calculators are being used in the development of a significant new radio signal processing capability.

Microphones. Reducing microphone size would be of little significance because it is not a limiting factor in the size of future eavesdropping devices. Improvements in microphone performance, however, and in microcomputer audio processing and

noise filtering techniques will lead to improvements in audio surveillance device capability.

Recorders. Both the performance and size characteristics of recorders can be expected to improve in the future due to advances in audio processing, mechanical design, and recording tape materials. It has been found that signal processing technology, again supported by microcomputers, can condense human speech to store more information in a given length of recording tape. Improvements in mechanical design should permit size reduction and more precise control of the recording tape drive mechanism; and common, magnetic plastic tape should become narrower, thinner, and stronger. Cumulatively, these advances will bring about recording devices which are much smaller than today's cigarette package size eavesdrooping radio transmitters and will operate for several hours or days with built-in voice control actuators. Because of this impending decreased size, recording devices may be used in lieu of body transmitters except in those situations where continuous communication with others is essential.

CONCLUSIONS

Based on the stated findings, the following conclusions were drawn with regard to the present level of eavesdropping activity, the availability of supportive electronic devices, and the current legal structure.

Audio Eavesdropping Devices

Telephone Systems. It is concluded that:

1. It would be very difficult to control the practice of wiretapping by controlling the availability of equipment employed in the procedure since not all are uniquely identifiable as eavesdropping devices.

2. It would be virtually impossible to control the availability of those standard electronic parts which can be installed within the telephone instrument to convert it into a room eavesdropping device.

3. It may be possible to control the availability of inexpensive audio burglar alarm devices which can be used for room eavesdropping without modification.

Microphones. It is concluded that no control over the availability of microphones is necessary because of their fundamental position as a component in a vast, commercial market.

Radio Transmitters. It is concluded that:

1. The availability of inexpensive radio transmitters offered to the public under the guise of wireless microphones can be constrained without undue, adverse effects on the private sector.

2. Control over the availability of industrial communications and amateur radio equipment is unnecessary and undesirable, but that consideration of methods to prevent equipment modification for eavesdropping purposes warrants study.

3. No controls exist over the publication of instructions, schematics, or diagrams relative to fabrication of radio eavesdropping devices.

4. Better public knowledge and legal definition is necessary to improve practices of manufacturing, marketing, and advertising of radio transmitters.

Optical Systems. It is concluded that control is unnecessary and undesirable over optical equipment availability because of the wide commercial use of laser and other light beam devices.

Recording Devices. It is concluded that no further control is necessary or desirable regarding the availability of conventional recording equipment.

Countermeasures

Based upon observations made during this study and the data reviewed in the countermeasures product and service area, it is concluded that:

1. Equipment performance claims by manufacturers are often ambiguous or frequently misleading to both the technical and non-technical customer in the public and private sectors.

2. The quality of debugging or technical security inspection services offered by security organizations varies widely and that minimum standards or statements of performance are infrequently offered or requested.

Interception of Non-Audio Information

It is concluded that under Title III there is no current, effective constraint relative to the availability of equipment or employment of procedures directed to the interception of non-audio information including computer data, satellite and microwave communications links, or information processing machines. There appears to be no reason why protections afforded by Title III should not be extended to encompass interception of non-audio information.

Aids to Physical Surveillance

It is concluded that no control exists under Title III over the physical surveillance devices market because all known manufactured electronic devices are not used for privacy invasion of a clandestine, audio information gathering nature.

RECOMMENDATIONS

Guided by the conclusions drawn during this study, it is recommended that actions be initiated to improve protections afforded the private citizen by:

1. The licensing of surveillance devices manufacturers.

2. The licensing of counter-surveillance or debugging equipment manufacturers.

3. The licensing of individuals or firms who offer to sell the services of counter-surveillance sweeps or debugging.

4. The reduction in availability of disguised devices sold or offered for sale through misrepresentation as under the guise of innocent devices such as "burglar alarms" or "baby monitors".

5. The preparation, dissemination, and fostering of guidelines for law enforcement personnel which provides instruction in the characteristics, handling, and identification of suspect electronic eavesdropping devices; the characteristics and use of countermeasure products and services; and the use and limitations of electronic surveillance.

6. The expansion of Title III legislation regarding the terms and definitions used to describe electronic surveillance devices that includes prohibition of interception of non-audio information and its acquisition through use of electronic devices.

7. The prohibition of publication for distribution of schematics, diagrams, and instruction manuals for the fabrication of eavesdropping devices.

A brief discussion in support of each recommendation follows:

Licensing of Surveillance Device Manufacturers

Current legislation restricts the acquisition of electronic surveillance devices generally to officials of law enforcement and communications common carriers. It lends little support to improving the quality of equipment offered by legitimate electronic device manufacturers. This forces the surveillance equipment prices upward since the producer is prohibited by statute from stockpiling components, engaging in the research and development of better equipment, and assembling and distributing electronic surveillance devices according to normal commercial practices. That is, a manufacturer cannot inventory, mass produce, demonstrate, distribute or promote electronic eavesdropping equipment or offer support services. As a result, new ideas for better products which might allow more effective law enforcement, lower prices, and better quality, are suppressed from entering the legitimate market. Aggravating this situation, according to some manufacturers, is unequal enforcement of the existing law which seemingly permits a few manufacturers to stockpile partially assembled devices and thereby manipulate or avoid the intention of the law. This causes unfair competition among the legitimate and the unethical manufacturers and tends to degrade the character of the entire market. This atmosphere is so severe that several well-known manufacturers of miniature, body bug transmitters currently use designs and techniques that are ten years old. Analagous devices produced in Europe frequently exhibit better performance, smaller size, and better reliability because of the absence of strict control.

It is recommended that electronic surveillance device manufacturers be licensed. Implementation of this recommendation will allow qualified manufacturers to produce surveillance equipment economically in a carefully controlled environment, thereby providing a means for improving the quality of devices, reducing costs, and stimulating growth and improvement in the overall market without fostering an increase in illegal activity.

Licensing of Counter-Surveillance Equipment Manufacturers

The licensing of countermeasures or debugging equipment manufacturers is long overdue, since the technical security marketplace has been plagued for years by claims of miraculous "bug" or "tap" detecting devices. These far reaching claims border on fraud; but currently there is no effective mechanism to restrict advertising since neither equipment performance standards nor a capable governing body exists to review these claims.

Implementation of this recommendation would provide a means for limiting fraudulent practices by establishing a regulatory licensing structure under the auspices of a standards laboratory that generates and maintains adequate technical standards. These governing standards and licensing arrangements could be structured in a three-tiered heirarchy to provide basic minimum performance levels for equipment in the private sector, a higher level for the law enforcement and industrial sector, and a top level for the most sophisticated customers. The countermeasures equipment advertised and sold would be graded according to measured performance, and public display of this record or certificate would be required in advertising and on equipment offered for sale.

Licensing of Countermeasure Service Organizations

Practitioners of "debugging" or countermeasures sweep services offer a wide range of capability for an equally wide range of prices. These service organizations may charge for services performed which are completely undefined, unstandardized and uncontrolled. Many other commercial service organizations are required, through self-policing actions of trade associations, by regulatory bodies of government, or by statute, to guarantee specific levels of proficiency in the performance of services.

By implementation of this recommendation, improved consumer protection would be effected. A rating, based on licensing examination of the service organization, would be required by reputable service firms and provide the customer with confidence in the quality and cost of services procured.

Availability of Disguised Devices

Readily available, inexpensive electronic devices such as wireless microphones, baby monitors, and telephone controlled audio burglar alarms can be easily converted to audio eavesdropping devices. Usually, the performance of these units can be greatly improved by increasing the number of batteries used or lengthening the antenna.

Implementation of this recommendation would control the availability of devices in this market by requiring new fabrication techniques to prevent device modification, disassembly, retuning, or power increase.

Training of Law Enforcement Personnel

No standard procedures are available to private citizens or police organizations which can be relied upon for credible guidance in the event of discovery of a suspected eavesdropping device or practice which could result in an electronic invasion of privacy.

Implementation of this recommendation provides for the creation of procedural guidelines for police and law enforcement officials to improve the enforceability of current and anticipated laws. By establishing a mechanism through which the technical characteristics of an electronic device may be examined, by assuring that guidelines are developed, disseminated and publicized so that electronic surveillance devices and countermeasures may be made available for proper use by law enforcement personnel, and by training of these personnel when necessary, the use and limitations of electronic surveillance technology can be better understood by law enforcement personnel. Through this enhanced understanding, the private citizen can be assured of competent protection by qualified police assistance.

Interception of Non-Audio Information

The terminology of the Title III statute and the rapid growth in electronics technology has combined to bring to the public attention the lack of coverage provided by the legislation. In practice the eavesdropper has skirted the intent of the law by assembling electronic devices in modular form so that the connection of sub-assemblies results in complete formation of an eavesdropping device. It is recommended that further study be devoted to this problem with the idea of making such assemblages of equipment, due to their existence together and the knowledge that in a precise configuration the modules create an eavesdropping device, presumptive of intent to use the modules for eavesdropping.

Further, it is recommended that a review of terms and definitions in the Title III legislation result in clarification of such word usages as "oral", "aural", or "communication". Without specific reference to Title III context, it is suggested that the concept of "intercept" of "communication" be expanded to encompass all clandestine interception of communications of an oral or non-oral nature.

Publication of Eavesdropping Device Literature

Numerous eavesdropping devices are described in literature that is readily available to the public. These publications are often completely descriptive of device circuitry including design drawings, schematics, parts lists, techniques of fabrication, and integration for system application. These documentation packages are usually offered for sale with no less intention than encouragement to the recipient of the information to manufacture illegal devices.

Implementation of this recommendation would inhibit the dissemination and proliferation of specific data where its utilization may result in Title III violations.

B. Civil Liberties Issues and Policy

AMERICAN BAR ASSOCIATION PROJECT ON
STANDARDS FOR CRIMINAL JUSTICE

STANDARDS RELATING TO

Electronic Surveillance

Recommended by the

SPECIAL COMMITTEE ON STANDARDS FOR
THE ADMINISTRATION OF CRIMINAL JUSTICE

William J. Jameson, *Chairman*

and the

ADVISORY COMMITTEE ON THE POLICE FUNCTION
(as of June, 1968)

Richard B. Austin, *Chairman*
G. Robert Blakey, *Reporter*

March 1971

The standards as set forth in this supplement were approved by the House of Delegates on February 8, 1971. This supplement is substantially in the form in which the proposed final draft was submitted to the House.

Introduction

At the same time that the Advisory Committee on the Police Function was formulating standards relating to electronic surveillance, the Congress was working along the same lines on federal legislation dealing with similar matters. The federal legislation was enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (P.L. 90-351) during June 1968, the same month as the publication of the Advisory Committee's Tentative Draft. Since then two Annual Surveillance Reports, entitled "Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications," have been transmitted to the Congress by the Director of the Administrative Office of the United States Courts, as required by Title III. These Reports, in the judgment of the Special Committee, bear out the views of the Advisory Committee as to the desirability of electronic surveillance as a law enforcement technique and as to the efficacy of the imposed restraints in maintaining the use of such techniques within limits tolerable in a free society. In addition, as the cases developed by these techniques have moved along in the judicial process, two federal district courts, one in Florida and one in the District of Columbia, have recently upheld the constitutionality of several key provisions in Title III;* and no court has yet held them to be unconstitutional.

Upon the recommendation of the Council of the Section of Criminal Law, the Special Committee proposed revisions of the Tentative Draft standards which largely would bring them into closer conformity with the provisions of Title III and which, therefore, do not work substantial change. The standards, with these revisions, were supported by the Advisory Committee on the Police Function (as constituted in June 1968),† the Council of the Section of Judicial Administration and, so far as they went, the Criminal Law Council.

---

*See United States v. Escandar, 8 Crim. L. Rptr. 2121 (S.D. Fla.; dec'd 11/2/70); United States v. Tantillo, Crim. Case No. 1912-69, D. Col.

†The proposed revisions were submitted for comment to the Advisory Committee as it was constituted when the standards were formulated.

The Criminal Law Council, however, proposed further amendments, which were the subject of debate when the standards were submitted to the House of Delegates for its approval at the February 1971 Mid-Year Meeting.

The further amendments proposed by the Criminal Law Council were submitted in the form of three motions: one dealing with disclosure of transcripts of overheard communications, one dealing with use of evidence obtained under the exercise of the President's powers regarding national security, and one dealing with emergency and lengthy surveillances. The texts of the proposed amendments are set forth in an appendix to this Supplement, *infra*.

The *disclosure* motion had two branches. One branch dealt with pretrial notice of the use of overheard communications as evidence. Section 2.3 (b), as revised by the Special Committee, requires disclosure of electronic surveillance information in accordance with the ABA Standards Relating to Discovery and Procedure Before Trial. The Criminal Law Council sought to substitute a standard requiring disclosure at least ten days in advance of trial. While there was no disagreement in principle, the Criminal Law Council believed that the matter should be specifically covered in this report and the Special Committee thought it more appropriate to leave treatment of the subject to the more comprehensive Discovery report already approved by the House. The second branch of this motion dealt with the standards relating to inventory of court-authorized surveillances, an auditing device designed to maintain visibility of the process. Section 5.15 requires notice to interested persons of facts pertinent to the surveillance other than the content of intercepted communications; section 5.16 deals with permissible disclosure of the communications—only by a law enforcement officer to another in the performance of his duties or in a court or grand jury proceeding, unless good cause is shown therefore before a judicial officer. The Criminal Law Council would have added a new section after 5.15 mandating disclosure, upon request, of the contents of the communications to all persons served with the inventory, on the ground that such disclosure was necessary to permit raising the issue

of unlawful surveillance. The Special Committee argued that the court needed discretion in order to deal appropriately with the case where a person served with the inventory is not a party to the communication, *e.g.*, only the proprietor of the premises, and where one of the parties has a legal privilege against disclosure. The motion was defeated by a vote of 127 to 104.

The *national security* motion sought to prohibit the use in evidence of communications overheard under the President's power to authorize use of electronic surveillance to protect the nation from hostile acts of foreign powers and from foreign intelligence activities (section 3.1). While recognizing that the President may have the right to authorize such surveillance without court approval, the Criminal Law Council argued that there is no such exception permissible under the Fourth Amendment, and, since the methods required by *Berger*, 388 U.S. 41 (1967), and *Katz*, 389 U.S. 347 (1967), would not be met, the evidence could not be used in a criminal prosecution. The Special Committee argued that the issue had not yet been squarely faced by the Supreme Court and supported the use of such evidence, as provided in section 3.2, on the ground that, if the overhearing was constitutionally within the President's powers, the seizure was not unreasonable under the Fourth Amendment, and there was no constitutional purpose served in excluding the evidence thereby obtained. The motion was defeated by a voice vote.

The *emergency and lengthy surveillance* motion sought to bar emergency surveillances without prior court approval (deleting section 5.2) and to restrict the length of time a particular surveillance could be authorized to five days, with one five-day extension (deleting section 5.4 and amending section 5.9). The Criminal Law Council argued that surveillances conducted without prior court approval and longer court-approved surveillances than those recommended were unreasonable invasions of privacy and, moreover, were already prohibited under the Supreme Court's decisions in *Berger* and *Katz*. The Special Committee argued that *Berger* and *Katz* did not have to be read as narrowly as the reading urged by the Criminal Law Council and that the scope of surveillance authorized

by the standards (and Title III of the federal statute) was necessary to be feasible, and was not unreasonable under the various safeguards required, *e.g.*, that the emergency surveillance meet the test required for the court to authorize an ordinary surveillance if the evidence obtained is to be admissible, that probable cause be shown for the initial 15-day period and any 30-day extensions authorized by the standards. The motion was defeated by a voice vote.

Additional exposition of the Criminal Law Council's views may be found in its report to the House of Delegates at the February 1971 Mid-Year Meeting. Further discussion of the Special Committee's position is contained, generally, in the commentary in the Tentative Draft of June 1968 and, more specifically, in the commentary to the sections involved, *infra*.

One member of the Special Committee, Arthur J. Freund, requested that his vote in opposition to the promulgation of any standards in this area be specifically recorded. Mr. Freund's dissenting views are set forth at the end of the standards and commentary, *infra*.

The standards and commentary which follow are set forth in the form in which they were submitted to the House of Delegates.

PART I. GENERAL PRINCIPLES

1.1 Objectives; prohibition; exception.*

(a) Objectives; privacy; justice.

The objectives of standards relating to the use of electronic surveillance techniques should be the maintenance of privacy and the promotion of justice.

(b) Prohibition; public; private.

Except as otherwise expressly permitted, the use of electronic surveillance techniques for the overhearing or recording of wire or oral communications uttered in private without the consent of one of the parties should be expressly prohibited. Subject to limitations of constitutional power and considerations of federal-state comity, the prohibition should be enforced with appropriate criminal, civil, and evidentiary sanctions.

(c) Exception; public.

Subject to strict statutory limitations conforming to constitutional requirements, [law enforcement officers in the administration of criminal justice] the Attorney General of the United States, or the principal prosecuting attorney of a state or local government, or law enforcement attorneys or officers acting under his direction should be permitted to use electronic surveillance techniques for the overhearing or recording of wire or oral communications uttered in private without the consent of [the parties] a party only in investigations of the kinds of criminal activity referred to in sections 3.1 and 5.5 of these standards. The limitations should be enforced through appropriate administrative and judicial processes.

---

*The standards are reproduced as originally proposed by the Advisory Committee. Material which is recommended for deletion is placed in brackets. Material which is recommended for addition is underlined.

Commentary

These amendments are designed to reflect the relationship between the general principles and the specific standards. No change in substance is intended.

PART II. SANCTIONS

2.1 Criminal sanctions.

(a) Penalty.

Except as otherwise permitted under these standards, [all aspects of] conduct as specified in this section relating to the use of [electronic surveillance techniques] a mechanical, electronic or any other device for overhearing or recording of wire or oral communications uttered in private without the consent of [the parties] a party should be made criminal or regulated.

(b) Scope; overhearing; recording; use; disclosure; devices.

The [prohibition] legislation should include—

(i) prohibition of the intentional overhearing or recording of such communications [so overheard or recorded] by means of such a device;

(ii) prohibition of the intentional use or disclosure of such communications so overheard or recorded or evidence derived therefrom;

(iii) prohibition of the intentional unauthorized use or disclosure of such communications otherwise lawfully so overheard or recorded or evidence derived therefrom;

(iv) regulation, backed by criminal sanctions, of the [intentional] possession, sale, distribution, advertisement or manufacture of a device the design or disguise of which makes it primarily useful for the surreptitious overhearing or recording of such communications;

(v) prohibition of the intentional promotion, whether by advertising or otherwise, of any device [where the advertisement

promotes the] for unlawful use [of the device] in overhearing or recording such communications; and

(vi) a provision for the confiscation of any overhearing or recording device possessed, used, sold, distributed or manufactured in violation of the prohibition or regulation.

[A good faith mistake of fact or law should constitute a defense to criminal liability.

Consistent with the standards in Parts IV and V, law enforcement officers, or those under contract with them, acting in the proper performance of their official duties, or in fulfillment of their contract, should be excluded from the prohibition.]

(c) Enforcement; immunity.

The prohibition, where necessary, should carry with it provision for the granting of immunity from prosecution in the investigation of violations of it.

Commentary

The amendments to subsection (a) and the first paragraph of subsection (b) are designed to clarify the scope and intent of the standard. The paragraph as to mistake is deleted in order to leave the matter to applicable principles of substantive criminal law. The last paragraph is deleted because it proved to be a source of misunderstanding as to the scope of the law enforcement exception, which is set forth in other standards, and is a matter of detail in any event, to be taken care of in any implementing legislation. The omission of this explicit provision is not intended as a change of substance.

2.2 Civil sanctions.

(a) Cause of action.

Except as otherwise expressly permitted, the use of electronic surveillance techniques for the overhearing or recording of wire or oral communications uttered in private without the consent of [the parties] a party or the use or disclosure of such communications or evidence derived therefrom, knowing or having reason to know that such communication or evidence was so obtained, should give rise

to a civil cause of action against any person or governmental agency who so overhears, records, or [knowingly] discloses or uses such communications or evidence derived therefrom, or procures or authorizes another to do so.

(b) Defense; court order.

Good faith reliance on a court order or other legislative authorization should constitute a complete defense to civil recovery.

Commentary

The first amendment reflects the decision of the Special Committee regarding consent under section 4.1 to parallel the standards to the provisions of Title III of Public Law 90-351, noted below. The second amendment merely makes explicit the principle that the standard would also apply to procured or authorized surveillance.

2.3 Evidentiary sanctions.

(a) Suppression.

Except as otherwise expressly permitted under these standards, [No] no wire or oral communication uttered in private and overheard or recorded without the consent of [the parties] a party [except as otherwise expressly permitted], or evidence derived therefrom, should be received in evidence in any trial, hearing or proceeding in or before any court, grand jury, department, officer, agency, regulatory body or other authority,

(b) Pre-use notice [; waiver] in criminal cases.

[No such communication so overheard or recorded, except as otherwise expressly permitted, or evidence derived therefrom should be received in evidence in or before such court, department, officer, agency, regulatory body, or other authority unless within ten days before such trial, hearing or proceeding the party offering such communication or evidence derived therefrom furnishes other interested parties copies of the relevant portions of the records of the communications, the court order, and accompanying applications under which the overhearing was authorized or approved. Where a failure to furnish parties copies of such records, orders and applica-

tions was not culpable or will not work prejudice, the communication or evidence derived therefrom should be admissible in the exercise of the sound discretion of the appropriate authority.] The standards set forth in ABA Standards Relating to Discovery and Procedure Before Trial should apply to disclosure by the prosecution in a criminal case of information relating to use of electronic surveillance techniques and to evidence derived therefrom.

(c) Motion to suppress; time; appealability.

Any party aggrieved by the overhearing, recording, use or disclosure of such communications or evidence derived therefrom so overheard, recorded, used or disclosed otherwise than as expressly permitted should be permitted to move to suppress such communications or evidence derived therefrom. The motion should be made prior to the trial, hearing or other proceeding unless there was no opportunity to make the motion or the party was unaware of the grounds on which the motion could be made. Where such a motion is made and granted, prior to the attaching of jeopardy, during the course of a criminal prosecution, the prosecutor, where necessary, should be afforded a right of appeal provided that the appeal is not taken for the purpose of delay and is diligently prosecuted.

[(d) Substantial rights; excusable error.

An error not affecting substantial rights in an application, authorization, or overhearing or recording of the otherwise authorized overhearing or recording of wire or oral communications should not be grounds for the suppression of such communications or evidence derived therefrom. Excusable error made in the process of securing authorization for the overhearing and recording of such communications should be subject to cure by judicial ratification.]

Commentary

The amendment to subsection (a) reflects the change regarding consent in section 4.1.

The substitution of a cross-reference to the Standards Relating to Discovery and Procedure Before Trial for former subsection (b) leaves the matter of disclosure to development by the courts, since

those standards only require notice to the defense that electronic surveillance has taken place. This change reflects the unanimous judgment of the Special Committee that no decision need be taken in the context of these standards which would approve or disapprove the Supreme Court's decision in Alderman v. United States, 394 U.S. 165 (1969), holding that after "standing" (who may object) and "illegality" (was there an unlawful search) have been determined, *all* government files must be disclosed to the defense in order that the issue of "fruit of the poisonous tree" (what must be derivatively suppressed) may be litigated in the context of an adversary hearing. The Congress recently passed legislation that would set aside the *Alderman* decision (Title VII of the "Organized Crime Control Act of 1970"). The Congress has taken the position that *Alderman* is not of constitutional dimension, that is, that it is a supervisory opinion and that it is unwise. See S. Rep. No. 91-617, 1st Cong., 1st Sess. at pp. 62-70 (1969). The Criminal Law Council, in contrast, has urged that the *Alderman* decision is of constitutional dimension and that it reached the right result. It should be noted that the ABA Board of Governors, on July 15, 1970, in endorsing in principle the provisions of the Organized Crime Control Act and urging their enactment as soon as possible, approved Title VII and suggested the following:

> To amend Title VII, Part B, Section 702(a), in order to provide for a more restricted disclosure of evidence to the defendant as provided therein, by permitting the prosecutor to make a written request for an *in camera* screening by the court when he believes that such disclosure would constitute situations enumerated in Part A, Section 701, for example, those which would affect the security of the United States, endanger the lives and safety of informants, Government agents or others, or cause unjustified harm to the reputations of third persons; and to grant discretion to the court to withhold any such information deemed justified by its *in camera* examinations.

By a divided vote of 7-5, the Special Committee decided to omit subsection (d) on the grounds, urged by the Criminal Law Council, that these matters are best handled on a case-by-case basis and need not be stated in the text of the standards themselves.

It should be noted that, where the communication itself is to be

used in evidence at the trial, it must, under the Discovery standards, be disclosed to the defense prior to trial, like all other evidence to be used at the trial, under procedures set forth in considerable detail in those standards.

PART III. NATIONAL SECURITY

3.1 Counter intelligence; supervision.

The use of electronic surveillance techniques by appropriate federal officers for the overhearing or recording of wire or oral communications to protect the nation from attack by or other hostile acts of a foreign power or to protect military or other national security information against foreign intelligence activities should be permitted subject to appropriate Presidential and Congressional standards and supervision.

3.2 Use; disclosure.

Such communications so overheard or recorded, or evidence derived therefrom, should be received in evidence in any federal or state trial, hearing or proceeding in or before any federal or state court, grand jury, department, officer, agency, regulatory body or other authority where the overhearing or recording was reasonable. Other use or disclosure of such communications or evidence derived therefrom should be limited to the use or disclosure necessary to achieve the purpose of the overhearing or recording or on a showing of good cause before a judicial officer.

Commentary

The Criminal Law Council proposed an amendment to this standard, which the Special Committee rejected by a divided vote of 9 to 3, requiring compliance with other standards mandating prior judicial approval before the product of electronic surveillance, conducted by the President in the interest of the safety of the nation, could be utilized

in evidence in any judicial or other proceeding. The Special Committee rejected any reading of the Fourth Amendment that would invariably require compliance with a court order system before surveillance in the interest of the national security could be termed constitutionally "reasonable.". The constitutional propriety of national security surveillance outside of the court order system was specifically left open by the Supreme Court in *Katz*, 389 U.S. at 385 n. 23. In addition, the provisions of Title III of Public Law 90-351 recognize, at least obliquely, the possible propriety of the exercise of this power of the President as Commander-in-Chief and impose under federal law only a requirement of ad hoc reasonableness before the product of such surveillance can be used in any trial or other proceeding. Finally, it is noted that the issues involved in this problem are now in litigation in the courts and should be resolved by the Supreme Court in the not-too-distant future. Until such time as the Court squarely prohibits either the use of the techniques or excludes their product in court, the Special Committee was reluctant to approve any standard that might unduly circumscribe, even indirectly, the power of the President to protect the national security interest or to suggest that what is constitutional for the Commander-in-Crief to do under one provision of the Constitution could somehow be termed constitutionally "unreasonable" under the Fourth Amendment.

PART IV. OVERHEARING OR RECORDING WITH CONSENT

4.1 Overhearing or recording.

The [use of electronic surveillance techniques by law enforcement officers for the] surreptitious overhearing or recording of a wire or oral communication[s] with the consent of, or by, one of the parties to the communication should be permitted, unless such communication is overheard or recorded for the purpose of committing a crime or other unlawful harm.

79-064 O - 76 - 39

Commentary

This change represents a middle ground between the text of the original standard and the suggestion of the Criminal Law Council. Under the original standard, all private use of surreptitious recording techniques without the consent of *all* of the parties to a particular communication would have been disapproved. This reflects the law in some states. See, *e.g.*, ILL. ANN. STAT., ch. 38, §14.2. The Criminal Law Council suggested any recording with the consent of one of the parties should be permitted. The Special Committee decided, however, to follow the position of Title III of Public Law 90-351, which prohibits private recording where a specific intent to make the recording for the purpose of committing a crime or inflicting unlawful harm can be shown.

4.2 Authenticity.

When [the techniques should be so employed by] law enforcement officers engage in a recording practice permitted under section 4.1, they should employ devices and techniques which will insure that the recording will be insofar as practicable complete, accurate and intelligible. Administrative procedures should be followed under the supervision of the principal prosecuting attorney similar to those set forth in sections 5.13, 5.14 and 5.18.

Commentary

These amendments merely reflect the relationship between this standard and other relevant standards. No change in substance is intended.

PART V. OVERHEARING OR RECORDING WITHOUT CONSENT

5.1 Overhearing or recording; judicial order; authorized application.

The use of electronic surveillance techniques by law enforcement officers for the overhearing or recording of wire or oral communications uttered in private without the consent of [the parties] a party should be permitted upon a judicial order of the highest court of

general trial jurisdiction based on an [suitable] application in compliance with section 5.3 and authorized by the appropriate prosecuting officer, as described in section 1.1(c).

Commentary

These amendments merely reflect the relationship between this standard and other relevant standards. No change in substance is intended, other than to conform to the amendment of section 4.1.

5.2 Emergency situation.

The use of such techniques to so overhear or record such communications without a judicial order should be permitted where the law enforcement officer, specially designated by the appropriate prosecuting officer, as described in section 1.1(c)—

(i) is confronted with an emergency situation which requires such an overhearing or recording to be made within such time that it is not practicable to make an application and the emergency situation exists with respect to conspiratorial activities threatening the national security interest or to conspiratorial activities characteristic of organized crime;

(ii) determines that there are grounds consistent with these standards upon which an order could be obtained authorizing such an overhearing; and

(iii) makes an application setting out the facts constituting the emergency for an order of approval of the overhearing to a judicial officer within a reasonable period of time but not more than forty-eight hours after the overhearing has occurred or has begun to occur.

Where an application for approval is denied, all overheard or recorded communications should be treated as provided in 2.3(a) and an inventory filed as provided in 5.15. The denial of an order of approval should be made appealable.

Commentary

These amendments parallel the standard to the provisions of Title III of Public Law 90-351.

The Criminal Law Council, however, suggested that this standard and its implementing language in other standards should be rejected as inconsistent with the Supreme Court's dictum in *Katz*, 389 U.S. at 357-58. By a divided vote of 7-5, the Special Committee elected to follow the principle of emergency search announced in Carroll v. United States, 267 U.S. 132 (1925), and recently reaffirmed in Chambers v. Maroney, 90 S. Ct. 1975 (1970). It was the Special Committee's judgment that in a limited, but significant number of cases, it will be both possible and necessary to conduct limited, emergency electronic surveillance in a context where prior judicial approval is not feasible. See, *e.g.*, the fact situation in Desist v. United States, 394 U.S. 244 (1969). In the absence, therefore, of a determinative Supreme Court decision on the merits rejecting the application of the emergency principle in the precise context of this area, the Special Committee approved the principle of 5.2, with the limitation found in Title III.

5.3 Application; form; contents; additional facts.

An application for an order authorizing or approving the use of such techniques for the overhearing or recording of such communications should be made in writing upon an oath or affirmation and contain the following information—

(i) the identity of the prosecuting officer authorizing the application;

(ii) the identity of the law enforcement officer making the application;

[(ii)](iii) the identity of the person, if known, whose communications are to be or were overheard or recorded;

[(iii)](iv) a specification of the particular offense which is or was under investigation;

(v) a particular description of the type of communications sought to be or which were overheard or recorded;

[(iv)](vi) a particular description and the location of the facilities, if any, over which or the place where the communications are to be or were overheard or recorded;

[(v)](vii) the expected or actual period of time of the overhear-

ing or recording, and if the nature of the investigation is such that the authorization should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

[(vi)](viii) a complete statement of the facts relied upon by the applicant warranting the issuance of an order of authorization or approval; and

[vii](ix) a recitation of all facts concerning previous applications or overhearing or recording, known to the individuals authorizing and making the application, made in reference to the person whose communications are to be or were overheard or recorded and the facilities over which or the place where such communications are to be or were so overheard or recorded, including, where the application is for the extension of an order, a statement setting forth the results thus far obtained from the overhearing or recording or a reasonable explanation of the failure to obtain such results.

The judicial officer to whom the application is submitted should be permitted to require the applicant to furnish additional facts under oath or affirmation, which should be duly recorded.

Commentary

These amendments reflect the addition of language paralleling that appearing in Title III of Public Law 90-351. No change in substance is intended.

5.4 Probable cause; kinds of showings.

The statements of facts relied upon and submitted by the applicant should establish probable cause for belief that—

(i) (A) where the applicant expects or expected an extended period of overhearing or recording, the person is presently or was then engaged over a period of time in the commission of a

particular offense with two or more close associates as part of a continuing criminal activity; or

(B) where the applicant expects or expected a brief period of overhearing or recording, the person is or was committing, has or had committed, or is or was about to commit a particular offense at a specific time;

(ii) facts concerning [a] that particular offense could have been or may be obtained through an overhearing or recording from the facilities over which or at the place where such communications are to be or were overheard or recorded;

(iii) other investigative procedures have or had been tried and have or had failed or reasonably appear or appeared to be unlikely to succeed if tried or to have been or to be too dangerous.

Commentary

Clarifying language only has been added. No change in substance is intended.

The Criminal Law Council suggested, however, that this standard on probable cause be omitted and section 5.9 on time be modified. See below. It was their view that, in combination, these two standards permitted surveillance for a period of time beyond that constitutionally permissible under the Supreme Court's surveillance trilogy, cited above. The Special Committee decided, on the other hand, by a divided vote of 8-4, that these cases need not be read in such a restrictive fashion. In the judgment of the Special Committee the permissibility or impermissibility of extended surveillance and the appropriate character of the showing of probable cause justifying it should be evaluated on a case-by-case basis. See Stewart, J., in *Berger*, 388 U.S. at 69: "The showing of justification [must] match the degree of intrusion." What is to be sought, in the words of the Supreme Court, is not long or short surveillance, but that "no greater invasion of privacy [be] permitted than [is] *necessary under the circumstances*." *Katz*, 389 U.S. at 355 (emphasis added).

5.5 Designated offenses; criteria.

An application for authorization or approval should be permitted

only in the investigation of designated offenses. The offenses should be serious in themselves or characteristic of group criminal activity.

5.6 Other offenses; use or disclosure; time.

The use or disclosure of facts contained in an overheard or recorded communication relating to an offense other than the offense under investigation should be permitted where an application for an order of approval is duly made as provided in 5.3 which includes an additional showing that the overhearing or recording was or could have been otherwise authorized. An application for approval should, however, be permitted for the use or disclosure of facts relating to other than designated offenses. Where the application concerns an overhearing or recording made during a period of authorized overhearing or recording, the application should be made as soon as practicable. Where the application concerns an overhearing or recording made in an emergency situation, the application should be made within the period of time otherwise required by 5.2. The denial of an application for an order of approval should be made appealable.

5.7 Judicial discretion and determination.

The judicial officer to whom an application for authorization or approval is submitted should be permitted in the exercise of sound discretion to deny the application, [or] and should be authorized to grant the order as requested or with appropriate modifications only if he determines that there is probable cause as provided in section 5.4.

Commentary

Clarifying language changes not affecting substance have been made.

5.8 Order; form; contents.

The order should be issued in writing signed by the judicial officer and contain the following information:

(i) the identity of the prosecuting officer authorizing the application;

(ii) the identity of the agency to which authority to overhear or record or to which approval of overhearing or recording is granted;

(iii) the identity of the person, if known, whose communications are to be or were overheard or recorded;

(iv) a specification of the particular offense as to which overhearing or recording is authorized or was approved;

(v) a particular description of the type of communications sought to be or which was overheard or recorded;

[(v)](vi) a particular description of and the location of the facilities from which or the place where the communications are to be or were overheard or recorded;

[(vi)](vii) the period of time of authorized or approved overhearing as provided in section 5.9;

(viii) a requirement, where appropriate, for progress and need report as provided in section 5.9.

Commentary

These changes reflect parallel provisions in Title III of Public Law 90-351.

5.9 Time; termination; extensions.

No order should authorize or approve the overhearing or recording of communications for a period of time beyond that necessary to achieve the objective of the overhearing or recording warranted by the showing or probable cause as provided in 5.4(i)(A) and (B). An order of authorization should require that overhearing or recording begin as soon as practicable and terminate when the objective is achieved or, in any event, after fifteen days from the date specified in the order. Extensions of the order should be granted for periods of not longer than thirty days only upon proper showings of probable cause as provided in 5.4. No limit should be placed on the number of extensions which can be granted; but the court should be

authorized to require progress reports showing need for extended overhearing or recording at such intervals as it deems appropriate and, where appropriate, to terminate the order in the exercise of sound discretion.

Commentary

This amendment reflects parallel provisions of Title III of Public Law 90-351.

The Criminal Law Council suggested, however, that the period of authorized surveillance be sharply limited in time below that now authorized under Title III or which could be authorized under this standard, to wit, five days. This suggestion was rejected by the Special Committee, in part for reasons noted above under section 5.4. In addition, the initial experience of the Department of Justice under Title III, as reflected in the Annual Surveillance Reports, indicates that the fear of the Criminal Law Council that extended surveillance would necessarily result in a disproportionate interception of innocent communications has not been borne out in practice. For example, according to the Second Annual Surveillance Report, Federal Wiretap No. 9 in the District of Columbia was granted for 30 days, with one 14-day extension. It was in actual operation for 39 days. 5,889 intercepts were made, of which 5,594 were incriminating. This one wiretap resulted in the arrest of 26 persons, including a narcotics wholesaler, a corrupted policeman, and two alleged members of La Cosa Nostra, who were the New York importers. In light of this experience it was the judgment of the Special Committee that 5-day orders, as suggested by the Criminal Law Council, were neither practical in law enforcement terms nor necessary to protect privacy. Consequently, the original standards were approved.

5.10 Public facilities.

No order should be permitted authorizing or approving the overhearing or recording of communications over public facilities unless a[n additional] showing in addition to that required under sections 5.3 and 5.4 is made establishing probable cause for belief that—

(i) the overhearing or recording will be or was made in such a manner so as to eliminate or minimize insofar as practicable the overhearing or recording of other communications whose overhearing or recording are not or would not be authorized, and

(ii) there is or was a special need for the overhearing or recording of communications over the facilities.

Commentary

No change in substance is intended by the addition of this clarifying language.

5.11 Privileged communications.

(a) Facilities and places.

No order should be permitted authorizing or approving the overhearing or recording of communications over a facility or in a place primarily used by licensed physicians, licensed lawyers, or practicing clergymen or in a place used primarily for habitation by a husband and wife unless an additional showing as provided in 5.10 is made.

(b) Communications.

No otherwise privileged wire or oral communication [however] overheard in accordance with or in violation of these standards should [be disclosed or used unless it is necessary in the disclosure or use of other communications whose overhearing or recording was authorized or approved] lose its privileged character.

Commentary

The amendment of subsection (b) parallels the standard to provisions of Title III of Public Law 90-351. No change in substance is intended.

5.12 Orders and applications; custody; destruction.

All orders and applications should be maintained for ten years in such places as the judicial officer directs. They should not be disclosed or destroyed except on judicial order.

5.13 Authenticity.

(a) Electronic surveillance techniques employed by law enforcement officers for the recording of communications uttered in private without the consent of the parties should be so employed that a complete, accurate and intelligible record of the communication will be obtained.

(b) The contents of any wire or oral communication overheard by any means authorized by these standards should, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire or oral communication authorized under these standards should be done in such way as will protect the recording from editing or other alterations.

Commentary

New language from Title III of Public Law 90-351 has been added.

5.14 Return; record; time, sealing; custody; destruction.

As soon as practicable but not later than thirty days after the termination of the overhearing or recording, a return on the order of authorization or approval should be made to the judicial officer. The recordings of overheard communications should be sealed until such time as the recordings or evidence derived therefrom are to be received into evidence as provided in 2.3(b), except that duplicate recordings may be made for use or disclosure for investigative purposes or trial preparation under appropriate safeguards. The presence of the seal provided for by this section, or a satisfactory explanation for the absence thereof, should be a prerequisite for the use or disclosure of the contents of any wire or oral communication or evidence derived therefrom. The recordings should be maintained in such places and in such custody as the judicial officer directs for at least ten years and should not be destroyed except on judicial order.

Commentary

New language from Title III of Public Law 90-351 has been added.

5.15 Inventory; time; postponement.

As soon as practicable but no later than ninety days after the return is made to the judicial officer or the date of an application for approval provided for in 5.2, which was denied, the judicial officer should cause to be served on the person named in the order of authorization or approval or the application for such an approval and such other parties to the intercepted communication as the judicial officer may determine in his discretion that it is in the interest of justice to serve, an inventory which should include notice of—

(i) the entry of the order or the making of the application;

(ii) the date of the entry of the order or of the denial of the application;

(iii) the period of authorized, approved or disapproved overhearing or recording;

(iv) the overhearing or recording, if any, of communications; and

(v) the period, if any, of actual overhearing or recording.

Upon a showing of good cause made to the judicial officer, the serving of the inventory should be postponed.

Commentary

New language from Title III of Public Law 90-351 has been added. The Special Committee rejected the Criminal Law Council's suggestion to provide for fuller disclosure consistent with the Council's position on section 2.3 (b).

The Special Committee also rejected the suggestion of the Criminal Law Council that an arbitrary 60-day time limit be placed on the period during which the filing of an inventory might have been postponed, since it was felt that the determination of the proper period of postponement should be left to the case-by-case informed discretion of the judicial officer. In addition, it was the judgment of the Special Committee that too often 60 days would not be long enough to develop a sophisticated, complex criminal investigation from its street manifestations and to move it up through a chain of command to the major organized crime figures. Consequently, the Committee felt the auto-

matic notice requirement suggested by the Council would abort a significant number of important investigations long before they might have reached their ultimate objectives.

5.16 Disclosure; use

The disclosure or use by law enforcement officers of the contents of wire or oral communications [overheard or recorded without the consent of the parties] which have been obtained by means authorized by these standards, or evidence derived therefrom, should be permitted only to the extent it is in the proper performance of their official duties, provided that, when disclosure is involved, such disclosure is made only to law enforcement officers to the extent it is in the proper performance of their official duties to receive it. Any person, including law enforcement officers, should be permitted to make such disclosures while giving testimony under oath or affirmation in a criminal proceeding in any court or in a grand jury proceeding. Such communications or evidence derived therefrom should otherwise be disclosed or used only upon a showing of good cause before a judicial officer.

Commentary

Language from Title III of Public Law 90-351 has been added. No change in substance is intended.

5.17 Reports.

(a) Judicial reports; time; contents.

Judicial officers should make annual reports to an appropriate agency which should contain—

(i) the number of orders applied for;

(ii) the kinds of orders applied for;

(iii) the number of orders denied or granted as applied for or as modified;

(iv) the periods of time over which overhearing was conducted or recordings were made:

(v) the offenses specified in the orders or the applications which were denied;

(vi) the identity of the persons authorizing the applications; and

(vii) the identity of the law enforcement agency of the applicant.

(b) Prosecutive reports; time; contents.

Prosecuting officers should make annual reports to the agency specified in (a) which should contain—

(i) the information required in (a) (i)-(vii);

(ii) a general description of the overhearing or recording, separated by offense, including:

(1) the character and frequency of the incriminating communications overheard or recorded;

(2) the character and frequency of the other communications overheard or recorded;

(3) the number of persons whose communications were overheard or recorded; and

(4) the character and amount of the manpower and other resources used in the overhearing or recording;

(iii) the number of arrests resulting from the overhearing or recording;

(iv) the offenses for which the arrests were made;

(v) the number of trials resulting from the overhearing or recording;

(vi) the number of motions to suppress made, granted, or denied based on the overhearing or recordings;

(vii) the number of convictions resulting from the overhearing or recording;

(vii) the offenses for which the convictions were obtained.

(c) Public reports; time; contents.

The agency specified in (a) and (b) should make public a complete annual report based on the information required to be filed by (a) and (b).

5.18 Administrative regulations.

Law enforcement agencies should adopt administrative regulations, including standards, procedures and sanctions, dealing with the various aspects of the use of electronic surveillance techniques. The regulations, among other things, should—

(i) limit the number of agents authorized to employ the techniques;

(ii) specify the circumstances under which the techniques may be used, giving preference to those which invade privacy least;

(iii) set out the manner in which the techniques must be used to assure authenticity;

(iv) provide for the close supervision of agents authorized to employ the techniques;

(v) circumscribe the acquisition of, custody of, and access to electronic equipment by agents; and

(vi) restrict the transcription of, custody of, and access to overheard or recorded communications by agents.

Materials on the regulations should be incorporated into general and special training programs of the agency.

Dissenting Views of Arthur J. Freund, Member of Special Committee

As a member of the American Bar Association Special Committee on Standards for the Administration of Criminal Justice, I have opposed from the outset the formulation of any draft by the Special Committee on the subject of Electronic Surveillance and I dissent from the report of the Special Committee which has been presented for consideration by the House of Delegates. My dissent is based upon the strong conviction that the approval of any standards on Electronic Surveillance by the American Bar Association at this time would not be in the best interests of the Association and would detract from the excellent work of the Special Committee in so many vital and essential areas.

The Standards Relating to Electronic Surveillance are of unproven constitutional validity and, in my opinion, of doubtful desirability. Whether we like it or not, the Congress has adopted the Omnibus Crime Control and Safe Streets Act of 1968 (Public Law 90-341), which authorized in Title III, with some specific controls, electronic surveillance in the investigation of federal offenses. In matters involving important and serious criminal offenses and to protect our national security there is adequate applicable federal law. The main thrust of the Report on Standards of the Special Committee on Electronic Surveillance is to encourage the adoption of the standards by the several states and thus to encourage of the use of such methods at the state level. The recommended controls, I believe, are inadequate and in my judgment the enactment of state legislation on this subject is unnecessary and undesirable.

Wiretapping is an enormously serious assault upon our freedoms, our privacy and the fundamental values of our democracy. It is one of the hallmarks of a police state. The American Bar Association should stand aloof from giving its imprimatur to the adoption and extension of rules for the widespread use of devices which impinge upon the rights of a free people.

Many years ago, Mr. Justice Brandeis said in Olmsted v. United States, 277 U.S. 438, at 478 (1928):

> The makers of our Constitution . . . sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of the rights of man and the right most valued by civilized men.

It is in this spirit that I dissent from the report of the Special Committee in submitting for adoption by the American Bar Association its Standards Relating to Electronic Surveillance.

ARTHUR J. FREUND

St. Louis, Missouri
July 27, 1970

APPENDIX

Texts of Amendments Proposed by the Criminal Law Council

PART II. SANCTIONS

2.3 Evidentiary sanctions

(a) No change

(b) Pre-use notice; waiver (Substitute for present 2.3(b))

A party seeking to use as evidence private communications of others obtained by electronic surveillance techniques in any contested criminal or civil hearing or trial should be required to furnish within ten days of such hearing or trial to all interested parties copies of the complete transcript of the recordings of such overheard communication, any court order obtained and the supporting applications under which the overhearing was authorized or approved, subject to the court's power to issue protective orders safeguarding the interests of persons not named in the litigation.

In the absence of such notice, such evidence should not be admitted and the hearing or trial should be postponed for an adequate period of time to enable the interested parties to

79-064 O - 76 - 40

receive and review such transcripts of recordings and copies of any supporting court order and application.

(c) No change

PART III. NATIONAL SECURITY

3.2 Use; disclosure (Proposed substitute for present 3.2)

Such communications so overheard or recorded or evidence derived therefrom should not be received in evidence in any federal or state prosecution, except in compliance with the requirements contained in Standards 5.3, 5.7 and 5.8.

PART V. OVERHEARING OR RECORDING WITHOUT CONSENT

5.2 Emergency situation (Proposed that 5.2 be deleted)

5.4 Probable cause; kinds of showings (Proposed that 5.4 be deleted)

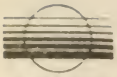
5.9 Time; termination; extensions (Proposed substitution for present 5.9)

The order of the court should specifically require that it be promptly executed and should not authorize the overhearing or recording of communications for a period of time beyond that necessary to achieve the objective of the overhearing or recording warranted by the showing of probable cause upon which the order is based, but in no event for a period longer than five days. Any application for an extension of the order for an additional period of five days should be made to fully comply with the requirements for initial applications set forth in 5.3 and for the issuing of a court order contained in 5.7 and 5.8.

5.16 Inspection following inventory (Note: This is a proposed new section which should logically follow immediately after the present 5.15 Inventory; time; postponement. Hence, the present 5.16 would become 5.17)

The judge upon the filing of an appropriate motion should make available to such persons referred to in 5.15, or their counsel, for inspection the intercepted communications, applications and orders identified in the inventory.

WILLIAM COLBY



THE C.I.A.

Secrecy in an Open Society

I would like to talk to you about what intelligence does for peace. The revelations of the past few weeks have probably led many of you to question what intelligence has to do with peace. Those revelations reflect things past, things that a new intelligence itself rooted out and corrected. We are now engaged in developing a new role for intelligence, one that reflects modern American precepts and values. We ask your cooperation and support in articulating this new role.

James Schlesinger once said that one of the primary social services expected from government is security. This can be gained, in the old Biblical phrase, by "a strong man armed in his camp." I think we have developed other ways to achieve security over the centuries, particularly in the past twenty-eight years during which American intelligence has matured and become the best in the world.

Intelligence now enables us to anticipate as well as to know. Anticipation allows us to arm ourselves, if such be necessary, with the right weapon. We need not face the light and accurate slingshot with an unwieldy broadsword. Anticipation also allows us to deter aggressors, demonstrating by our protective shield the futility of attacking us.

But anticipation these days also presents us with an opportunity, beyond anything known in the past, to negotiate. When we have knowledge of a foreign weapons system in the research phase, we can then discuss a mutual agreement to forgo its development and deployment. This can save millions of dollars on both sides — which can then be spent on plowshares rather than on swords. Such, of course, was the result of our negotiations with the Soviet Union about anti-ballistic missile systems. Intelligence made a significant contribution to the negotiating process, but its ability to monitor actual compliance was crucial to concluding the agreement. Vast sums, estimated between fifty and a hundred billion dollars, were saved because neither side had to build extensive ABM systems.

The anticipation made possible by good intelligence offers a greater contribution to peace than merely limiting weapons expenditures. Anticipating future disputes can permit their resolution while they are still only problems. Predicting crises and confrontations can permit conciliation and compromise before they occur. Suspicions and misunderstandings can be replaced by accurate perceptions that there are real problems on both sides. Men of good will can then work to resolve these problems through international conferences, through joint studies into the facts, or through recognition of mutual rights and interests.

I therefore believe it highly appropriate for intelligence to be invited to a discussion of how we obtain peace on earth. Intelligence has contributed to this end and will contribute even more in the future.

The problems of the future can result in conflict or cooperation. Consider:

- ☐ overpopulation and underproduction;
- ☐ nuclear proliferation;
- ☐ extremism and terrorism;

☐ the economic imbalances between rich and poor countries;

☐ the exploitation of hitherto inaccessible riches in the sea or in space;

☐ the interdependence of economies and even cultures;

☐ the acceleration of events by exponential improvements in transportation and communication.

We must have systematic knowledge of these complex subjects, full awareness of all our capabilities to deal with them, and an understanding of the intentions of the actors on the scene. Intelligence provides these. It is a tool to help America move toward peace with our fellow partners on this globe.

There are those, however, who contend that our intelligence has in the past and can in the future create the very problems that limit our hopes for peace. To them I say that their concept of intelligence is outmoded. When it looks at open societies, today's intelligence collects what is publicly available; uses technology to gather and process information that can be seen, heard, or sensed; and then carefully analyzes the bits and pieces of the jigsaw puzzles to provide an answer to the problems we face.

There are societies and political systems, however, that cling tenaciously to secrecy as a basis for power. Against these societies, which can threaten our peace, it is indeed necessary to employ the older techniques of secret intelligence developed for a world in which openness and free exchange were unobtainable. It is the very thought processes and procedures that create such secret plans that threaten our long-term hopes for peace among nations and peoples in the new open world we look toward.

We must avoid a repetition of our ingenuous belief during the nineteen-twenties that the world had been made safe for democracy and that gentlemen, in consequence, should not read other gentlemen's mail. If we can indeed achieve a world of gentlemen through the process of negotiation and resolution of the passions and ambitions of the past, then truly we can turn away also from the use of secret intelligence. But until that day, we hazard peace if we blind ourselves to realities, as the great democracies did during the nineteen-thirties.

The capability of intelligence quietly to influence foreign situations can contribute and has contributed to peace. I do not contest that many of these operations in our history were more narrowly justified by their contribution to what was then seen as America's interest.

But in a number of instances, some quiet assistance to democratic and friendly elements enabled them to resist hostile and authoritarian groups in an internal competition over the future direction of their countries. Postwar Western Europe resisted Communist political subversion, and Latin America rejected Cuban-stimulated insurgency. They thereby thwarted at the local level challenges that could have escalated to the international level.

That there can be debate as to the wisdom of any individual activity of this nature is agreed. That such a potential must be available for use in situations truly important to our country and the cause of peace is equally obvious.

Many of our citizens would express agreement with what I have said, but still express concern that there is an inherent contradiction between the need of intelligence for secrecy and our constitutional structure of openness. They reject a hypocrisy that allows intelligence to operate while professing that it does not.

It is true that the old concept of intelligence did conflict with our ideal of openness. This contradiction was dealt with by a cautious averting of responsible supervision from what were viewed as the necessary unpleasantries of the world of intelligence. The members of Congress who said they did not want to know of our activities, the careful circumlocutions used in the directives developed for intelligence — these reflected a consensus that while intelligence was needed to protect America, America was unwilling to admit its use of intelligence.

As a result, intelligence made some mistakes and did some misdeeds. That these were truly few and far between over the years of its history is a credit to the patriotism and integrity of the men and women of intelligence, rather than to controls upon them. But that they did occur forced attention to the need to articulate the proper role of intelligence in America.

After Vietnam and Watergate, exposures of improper intelligence activities aroused concern and launched the current exhaustive investigations. Intelligence has cooperated with these reviews because we in intelligence believe the future of intelligence is important to our country. We also believe that intelligence must find its fully understood and accepted position in our constitutional structure.

We Americans recognize the need for secrets when

our institutions cannot operate without them — witness our ballot box, our grand jury proceedings, and our protection of commercial secrets. Intelligence needs secrets or its agents are exposed; patriotic Americans contributing to their country are pilloried as fronts; and chinks in an adversary's armor are rapidly closed when we obligingly make them public.

We — all of us — must develop out of our current investigations a new concept of *responsible* American intelligence. It will be a further innovation that America can bring to the intelligence profession. We will do it in essentially three steps.

☐ We will articulate better guidelines for intelligence, spelling out what it properly can do and what it will not do. We will insure that it is focused on foreign intelligence, and does not infringe the rights of our citizens.

☐ We will develop better supervision of intelligence by the Executive, by the Congress, and even, where necessary, by the judiciary. Better external supervision of intelligence will certainly generate intensive internal supervision, insuring that American intelligence complies with America's constitutional concepts.

☐ And we will develop better secrecy for those aspects of intelligence that really need it, while at the same time ending the old tradition of total secrecy of everything about intelligence. The stream, even flood, of intelligence secrets that have been exposed this past year has brought home to every American the fact that we must have better protection for those secrets we need to keep.

Discussion

ANDREW YOUNG *(Member, U.S. House of Representatives)*: We talk as though the C.I.A.'s missteps were a thing of the past and that we do not intend to do these things ever again. But our proclivity to deal with people as clients and puppets rather than as friends and brothers makes it almost a foregone conclusion that we will repeat many of those mistakes.

We are involved right now in a war in Angola. It is known all over Africa that the United States has a military presence in Zaire supporting the F.N.L.A. [National Front for the Liberation of Angola] in Angola, although just how we are involved has never come before the Congress of the United States. We are on a side which doesn't make much sense in Africa because South Africa is also on that side. Yet, right next door, in Zambia, there is a man of integrity and enormous prestige, the son of a Presbyterian minister, who sounds like one of our founding fathers when he talks about the founding of his country. That is Kenneth Kaunda. Given our appreciation of the democratic process and our determination that people should have the right to make their own decisions and determine their own destiny, I would have thought we would have chosen to back men like Kaunda and Julius Nyerere of Tanzania, who say that all foreign influences should be withdrawn from Angola and that neighboring African leaders should help put together a coalition government.

Instead we chose the side in league with South Africa, and that puts us on the same moral level as that of the Soviet Union — that is, both superpowers are supplying weapons for blacks to kill blacks. It also extends the Cold War to Africa.

This kind of mistake after Vietnam and in the presence of the kind of debate that has been going on in both the House and the Senate tells me we have not yet learned what our American intelligence system should be.

Our intelligence system should respect emergent leadership in these countries and support the values of change and the democratic process. Covert, clandestine activity to preserve civilization is a contradiction in terms. Any civilization that is not built on trust and freedom is hardly worth the name civilization.

We do have to have intelligence to survive in this kind of world. But it is the gaps in accountability in a secret agency which must also be considered.

The hostile groups exposing our intelligence personnel, the hasty headlining of important technical intelligence projects, or the arrogance of those revealing our country's proper and important secrets in the cause of a self-proclaimed "higher morality," all these have demonstrated the weakness of our current procedures for protecting our necessary secrets.

We need no Official Secrets Act muzzling our press or frightening our citizens, and we in intelligence do not ask for one. We do need to be able to discipline those who freely assume the obligation of secrecy as members of our profession and then willfully repudiate it. We are sure that we can obtain the same recognition of our intelligence profession's need for confidentiality that we extend to our doctors, our lawyers, and our journalists.

Taking these three essential steps will not be easy. But I believe that we are now turning to a debate of the real issues that face American intelligence rather than agonizing over the missteps of the past. It is my sincere hope that this debate will lead to the kind of changes that I have outlined for American intelligence. It is vitally important to America that our citizens regain their respect and trust in our intelligence service. There must be a national consensus that American intelligence serves America and honors the Constitution. There must be a consensus that American intelligence is properly guided, properly supervised, and capable of protecting its own secrets so it can protect America.

I believe that a strong and free America is essential if we are to move toward peace on earth. I believe that a truly American intelligence service is equally essential to keeping America strong, free, and at peace.

Mr. Colby is the former director of the Central Intelligence Agency.

MORTON HALPERIN *(Senior Consultant, Center for National Security Studies; former Deputy Assistant Secretary of Defense):* It is clear that we need information about potential adversaries and potential dangers in the world. We need some kind of intelligence-gathering capability. But it is vitally important that we take the kind of steps Mr. Colby has suggested to bring that capability under control.

We need legislation by the Congress spelling out precisely what the intelligence agencies can and cannot do, and we need to back that up with effective laws making it a crime for those agencies to violate their charter. That would prevent a repetition of what one of Mr. Colby's predecessors did, which was to send a memorandum to the President's Assistant for National Security Affairs, telling him to treat the attached document carefully because it violated the C.I.A.'s charter, at which point both of them filed the document and went about their business.

The gathering and evaluating of evidence can be controlled by law. But it is an absolute delusion to think we can bring covert operations under democratic controls and make them conform to our democratic ideals. Covert operations are simply inconsistent with the American constitutional system and with the ideal we stand for in the world. The time has come for the United States to abolish its career service for covert operations and to make such operations illegal.

Now, both Senator Church and Mr. Colby have said that that cannot be done. Both hold before us the hypothetical horrible situation in which the future is said to depend on our preventing some group somewhere from seizing a nuclear weapon. Such a situation is highly unlikely; it is even more unlikely that the kind of covert capability we have maintained would be effective in meeting it. Moreover, Senator Church has already dealt with that problem in his committee report. He says that the President always has the right to take action when the survival of the United States does in fact depend upon it, and then to do what Abraham Lincoln did — come before the Congress and the people and say, "This is what I have done. You decide whether or not to ratify it."

The problem is that as long as we maintain a capability for covert operations and let our Presidents conduct them, they will use that capability in situations where they know they could not get public and congressional support.

Mr. Colby has asserted that the United States no longer conducts covert operations in free and open societies. This suggests a strained definition of free and open societies. It is now clear that we have covert operations in Portugal, in Angola, and in the Azores, and I would not define any of those societies as closed.

It is no accident that we resort to covert operations when they conflict with our ideals and would not be

supported by the Congress or the American people if they were known. There is no way in which you can bring covert operations under democratic control.

If we look at the kind of abuses that Senator Church's committee has been uncovering, and if we face them honestly, we must conclude that the only effective step we can take, one that is not at all inconsistent with our own survival, is to abolish covert operations.

RAY S. CLINE *(Executive Director of Studies, Georgetown Center for Strategic and International Studies; former Director of Intelligence and Research, Department of State, former Director of Intelligence, the Central Intelligence Agency).* In the nineteen-fifties and 'sixties, the C.I.A. and the intelligence agencies of the State Department and Department of Defense created the best intelligence system in the world.

I freely admit that in the twenty-eight years the C.I.A. has been in operation, some very serious mistakes were made. Some were made in the gray areas where guidelines were not adequate, because this was a new part of government, and so misinterpretations were possible. But the worst indiscretions were made by following direct orders from Presidents of the United States to become involved in internal security functions which were properly the task of other government agencies.

Leaving covert operations aside for the moment, and concentrating on intelligence gathering, we must have legislative and administrative remedies and a monitoring mechanism to prevent the excesses and aberrations which have been noted.

My fear and conviction is that this year-long bath of criticism of the intelligence agencies, particularly of the C.I.A., has nearly destroyed the effectiveness of the agencies in collecting information abroad. It has discredited and demoralized the people in the intelligence system, many of whom have not done anything except read newspapers and foreign intelligence reports and write scholarly essays and reports to the Congress, to the White House, to the State Department, to the Defense Department.

Furthermore, these criticisms have given the impression abroad that the C.I.A. is a criminal institution with which it is unpalatable to deal. I assure you we cannot operate effectively in the international arena if we destroy our own institutions.

For many years I have felt that Congress should establish a joint congressional oversight committee, composed of leaders from both the House and Senate, a committee which would concentrate on developing a national intelligence policy and the kind of intelligence institutions and programs we need. The new legislation should also clearly establish, more precisely than was done in 1947, that the intelligence community is a permanent part of the peacetime, decision-making, political process in this country, and it should have whatever guidelines and monitoring provisions are necessary. This would be an analytical service preparing reports, at various levels of secrecy, for the White House, the National Security Council, and the Congress. It would also be feasible for much of this work to be done for the public so that our communities of scholars could be introduced to the process through which they could come to an understanding of the complicated and dangerous world which exists around us.

The United States is in an exposed position. There is no great nation in the world which is not running a lot of intelligence-collecting operations against us. It would be imprudent if we shut our eyes and ears.

Regarding the nasty subject of covert political action, most people discuss that as if it were a social disease. The fact that every successive President has felt the need for some kind of covert political action in the interests of security ought at least to make us consider what its purposes are. Some of those purposes were misguided. I make no brief for, say, the Bay of Pigs operation. The secret Laotian army, after it became so large and paramilitary and almost overt, was not an appropriate clandestine function for the C.I.A. On the other hand, I regret the fact that a very small minority of the Laotian people have just deposed a centuries-old monarchy which was presiding over the fate of the most peaceful people in Southeast Asia until the North Vietnamese came in and organized a tightly disciplined paramilitary force.

There are places in the world where the United States has a responsibility to resist the establishing of one-party dictatorships, totalitarian societies, and paramilitary operations when the people in those countries do not want them and want our help. Senator Church has spoken properly of our country's great achievement in stabilizing Western Europe after World War II. The Marshall Plan was a distinguished economic achievement. NATO put a secure military cordon around that area, but if the Central Intelligence Agency had not been supporting the organs of free information and parliamentary political parties in Italy, France, and West Germany, the face of Western Europe would be quite different today because Russia was making strenuous efforts to create one-party dictatorships in those old democracies.

We should never legislate ourselves out of the possibility of coming to the defense of like-minded people around the world, quietly and secretly, by political assistance which usually means giving advice and money to people who are seeing their opponents armed and financed from outside the country in the interests of non-democratic societies.

I read the report of the Church committee and was a little nonplussed by one of its conclusions — that nobody got assassinated. The committee exposed the processes of government and named names to demonstrate that we had given serious thought to the possible assassination of Fidel Castro by Cubans at a time when the American policy was to send ashore a force of 1,600 armed Cubans to try to destroy Castro's whole regime. I am not sure that was a wise policy, but it does not surprise me that the government included in that policy the possibility of arming small infiltration bands as well as large paramilitary forces.

What does seem clear is that Fidel Castro is alive and well in Havana and that we need an intelligence system to carry on other parts of the business. I hope Senator Church's committee will give equal time to the achievements of the C.I.A. and the need for a good intelligence operation.

I am also a little distressed because Castro is sending thousands of armed guerrillas, organized by the K.G.B., the Soviet intelligence service, to assist in Communist revolutions in Portugal, in Angola, and, I am sure, in the Middle East.

It is important that we take every possible measure to support our kinds of institutions abroad. The C.I.A. has a small role to play in that kind of action, but it would be wrong if Congress made it impossible for future Presidents to use the C.I.A. in that role when it is appropriate and effective.

CHARLES MORGAN *(Executive Director, the American Civil Liberties Union)*: The function of the C.I.A. is the function of the Pinkertons. They are international company cops protecting, at a thousand American military posts around the world, our vital national interest, which is to say protecting American corporate interests. The reason, Senator Church, that we overthrew Mr. Allende in Chile, a democratically elected leader, is purely and simply because we had economic interests there. It is the same reason, I suppose, that we did not put in jail the man who offered a million-dollar bribe to a federal agency to overthrow Allende.

is the same reason why people in the F.B.I. did their work on Martin Luther King in the year when, I might add, we also began efforts to kill Patrice Lumumba. Senator Church's report well stated what Lumumba's problems were: he had "a magnetic public appeal and leanings toward the Soviet Union." Which, I suppose, in a reasonable world of democratically inclined people, a person has a right to have. According to J. Edgar Hoover, Martin Luther King had the same feelings.

The problem is not what we are discussing here. The problem is that we have an army that cannot win a war in the world, and we have a concept called democracy that we do not believe in because we cannot practice it at home. Imagine a country in which George Wallace and Ronald Reagan are sincerely thought of as Presidential candidates.

Wallace's slogan is "Trust the People." There's nothing wrong with that. Can Mr. Colby trust the people? Can the people trust Mr. Colby? And I do not fault you, Mr. Colby. For years I have paid you and you, Mr. Cline, and a government agency to lie to me and to Congress.

The entire population of the United States knows that its government lies. In a democracy that is a civil-liberties issue, because the people are entitled to be confronted with facts upon which to vote.

Covert activities require cover stories, and cover stories are a euphemism for lying. From cover stories to cover-ups in a city of cover-ups.

Gerald Ford wakes up on his last morning as Vice-President, walks out in front of his house, waves at the cameras, goes back inside and fixes his breakfast, then gets into his car and drives to work. From that day on, it has been all downhill, and the reason it has been all downhill is because the President of the United States, on the day he takes his oath of office, is obligated to lie. Covert activities require cover stories and cover stories. . . . It is implicit and inherent in the beast. Today, the revolutions of the world are fought against us. The poor of the world do not fight for us. We have not won anything since 1945. We gave it away to you, Mr. Colby, and I commend you for what you are doing with it; you are doing the best you can.

When Gerald Ford told the House Judiciary committee in his Vice-Presidency confirmation proceedings that there were things worth lying about, what he was saying, in effect, was that he did not have the luxury of not lying.

This is a city which lies, a city in which Jeb Stuart Magruder and Egil Krogh lie and then leave town and lecture the country on ethics.

The President of the United States is our national

teacher. When Harry Truman was President, children learned to play the piano. When Dwight Eisenhower was President, golf became a major sport. In a nation of liars, our President teaches that doctrine.

Covert activities are too costly. We must keep our satellites and our sensors, and we must hire scholars to analyze, of course, and we don't have to tell our trade secrets. But the spy in the Kremlin? Fire him, he costs too much. The wiretaps on the embassies? Unplug them, they cost too much.

And if the citizens of this country do not do that, then it will not be long before a Richard Nixon or a William Colby or a Gerald Ford, or whoever, will be ruling our lives.

CLAIBORNE PELL *(Junior United States Senator from Rhode Island)* Thank you for your strong statement. I think it is a little overstated. The United States is probably the most open government of any in the world. In going through this masochistic opening up of ourselves in recent months, it would be hard to find any government more open than ours. Obviously there have been cases of dishonesty in government. The majority of us can say with complete truth that we have been honest and have upheld the trust of the people, whether in the Executive or in Congress.

CHURCH: Of course, Mr. Morgan is right when he says that covert actions require cover stories and thus force Presidents from time to time into a position of lying. Covert actions are designed so that when the facts do surface, it will be possible for the President to "plausibly deny" any connection with the covert operation. That is where we get into such serious trouble. The point of my original remarks had to do with confining covert operations either to the imperatives of national survival or to the historic principles of our nation so that if the facts do surface, we will not have to lie about it. If, in fact, we help the people of Portugal, we can say yes, we helped them, eighty-five per cent of them want a democracy and the Russians were pushing in all kinds of money to impose a Communist regime with a military government. We can say we tried to help the democratic parties to stay alive, and we are proud of it. We do not have to lie about that, because our action conforms with our own principles and values.

Mr. Morgan said the government has developed a habit of lying, that the President, by virtue of the nature of covert actions, has been forced into lying, and that the Congress does not want to know the truth. Well, that has not been the habit of the committee it has been my privilege to chair. We determined that we would find out the truth and despite objections, even from the President, we have published the truth. I think that that is in the best traditions of this country.

Mr. Cline complains that that has demoralized and all but destroyed the C.I.A. It depends on your point of view. The other day I read the comments of two distinguished columnists about the work of our committee. One took Mr. Cline's line and said that because of our committee, the C.I.A. was in shambles. The other columnist said that our committee had dealt with the C.I.A. with such a velvet glove that we had all but abandoned our duty to conduct an honest investigation. I figured that morning that we might be doing it about right.

But, remember, this investigation began because of charges of most serious and unlawful wrongdoing directed, in some cases, against the American people and, in other cases, against foreign people, including certain foreign leaders. Those charges surfaced in the free press. Once they surfaced they had to be investigated. It was not this committee or the Congress that has caused whatever trouble exists in our intelligence agencies. It is their activities that were wrong. And the only way you are going to get them right is to get the facts out and make the necessary reforms. That is the way we as a nation have always done it, and that is what has made us a unique nation.

As far as moral certitude is concerned, I think all of us have enough of that to know the difference between a Portugal and a Chile, and to know the difference between the Greek colonels and the efforts to restore democratic government in Western Europe after World War II.

Mr. Halperin brings up a dilemma I have struggled with — which is, how can we be sure, if we have a secret apparatus and covert actions, that the agencies will conform to standards that the American people would approve if they knew about those actions? How can we be certain that Presidents will not abuse this power? Mr. Halperin says you can't, and so we must make all covert operations illegal. I have enough faith in our system to think we can control such operations. We must write definite restrictions into the law with respect to future covert operations.

In our report on assassinations, we have recommended adding to the criminal code appropriate provisions against conspiracies and attempts to assassinate foreign leaders. Other restrictions must be written into the law on covert operations.

Also, we must not leave it to the President to decide

Most of the things the C.I.A. has done and that the F.B.I. has done are things that our Presidents wanted them to do. — MORTON HALPERIN

about covert activities. The Congress has its responsibility. An appropriate joint committee of the Congress, informed and consulted with on all covert activities, would be the watchdog that could, together with the legal restrictions, keep covert operations within proper bounds. It is worth a try.

COLBY: Covert action can be brought under our statutes. Covert action has been undertaken by Presidents throughout our history. Benjamin Franklin was associated with a covert-action program in France designed to move weapons from France to some embattled colonists out in America without committing France to active participation in the Revolution. Most of us would probably consider that to be a proper covert operation.

We have also made some rather silly covert actions. President Grant once sent people up to Canada to try to entice some of the provinces to defect from Canada and join the United States. That was a rather conspicuous failure, but he thought he had the constitutional right to do it, and there wasn't much protest about it.

The Congress, of course, has faced this question of whether the United States should conduct covert activities. The Congress has been kept advised about covert operations in a variety of ways. Last year, both the House and Senate were asked whether we should abolish covert operations; specific bills were put up to that effect. Both houses said no, by a three-to-one vote. I will go with that.

I think most Americans feel that covert action is a weapon we must have in our national arsenal for use where it is appropriate. The question is, when is it appropriate? There is also the problem of plausible denial. Plausible denial was part of the mythology of early covert action. But when President Eisenhower at the time of the U-2 incident could not accept that kind of denial of Presidential responsibility, that was the death knell of the plausible-denial concept. I have pointed out to our employees that plausible denial is really no longer a viable theory, because it contradicts our American constitutional system and the responsibility that goes up to our senior leadership.

Regarding cover stories and lies, there is a distinction between telling a lie and refusing to talk about things you want to keep secret. This is a distinction we can make in America. I have said, and I have tried to stick to this, that I will not tell a lie to the American people and I will not lie to the Congress.

Regarding the wisdom, or lack of it, of our covert actions, President Kennedy once said that our successes are unheralded and our failures are trumpeted. Quite a few of our successes have come out, later, and are somehow put into a context in which they seem to be failures. The war in Laos is an example. I have always maintained that that was a success. A number of countries were interested in Laos. The North Vietnamese were moving troops in there, trying to take it over. About fifteen nations made an agreement in Geneva in 1962 that all would remove their forces and paramilitary forces from Laos and the country would remain neutral and independent. In a very few months, the North Vietnamese removed forty people and we removed about 1,500. The North Vietnamese left seven thousand there when they removed their forty. They then began to push the people in the Laotian hills around. President Kennedy was faced with a problem. Was he going to let this happen, or was he going to "send in the Marines"? He didn't want to send in the Marines, the Army, or anybody else, and he did not want to just sit and watch it happen. So he asked the C.I.A. if it could help. And the C.I.A. did help, for ten years. It committed a very large contingent of C.I.A. people to that operation — about two or three hundred officers. It spent a large amount of money, by C.I.A. standards, on that operation — in the tens of millions of dollars each year. At the end of ten years, the battle lines were about where they had

been when we started, although the North Vietnamese commitment had gone from seven thousand to seventy thousand.

I think that that was a pretty good story, because in the end, we achieved a coalition government and a neutral and independent Laos and a reassertion by all the parties that they would respect the independence and neutrality of Laos. Now Laos is a long way from the United States and you can debate whether that was in our national interest. But the C.I.A. did the job its government asked it to do. It did it effectively, and it made a contribution to freedom in that part of the world.

As for responsiveness of the agency to the American people on this sort of thing, the original act provided in 1947 that C.I.A. activities, other than intelligence gathering, had to be the result of a Presidential finding that they were important to the national security, and also that they had to be reported in a timely fashion to the appropriate committees of the Congress. There are six such committees. We are in full compliance with that act with respect to any activity the C.I.A. is performing anywhere in the world, outside of intelligence gathering. So this does provide a mechanism of deciding by the people's representatives in the Congress whether the kind of covert actions we undertake at any time are appropriate or whether they are a mistake.

PELL: I am sure that the audience is as struck as I am with one thought: How many nations would have their director of their secret intelligence agency appear on a panel of this sort? I would think you would not find this in any other nation.

MORGAN: Nor in this one until there were revelations untowardly made about that agency.

CLINE: The reasonable conclusion to be drawn from the fact that these representatives of the Congress and Director Colby of the C.I.A. are here at this table discussing these issues with remarkable candor is one which refutes the view that all the institutions of the American government are rotten and full of liars. I hope that Senator Church's committee and Congressman Otis Pike's committee will work with the Executive and, in full explanation to the people, figure out what kind of an intelligence organization we want and what we want it to do. The intelligence agencies have never been out of control. They have been following instructions, perhaps sometimes mistakenly when they should not have followed instructions. But if clear guidelines are presented thr representative legislation, I can assure you, from th years' experience working with this group — wi was patriotically motivated and protecting the inter of the country — that they will follow these prop constituted instructions from the government.

MORGAN: I don't think that all the institutions of American government are rotten. As a matter of f I think we ought to try some of them more of The Constitution of the United States provides a declaration of war. If we declare war, then should go to war, or we should aid other count openly and aboveboard. If another country c group in another country promotes democracy wants democracy — mind you, I am not talk about our "vital interests," be they Dean Ache or Dean Rusk's, or Henry Kissinger's, or Cap Exxon's — then why can't we openly fund country or group, discuss it, and talk about it? If are proud of them, we can do that.

Everyone in the U.S. government is not, of cou a liar. Some adopt, as Mr. Colby wisely does, approach of just not telling the folks. That certa beats lying, and the Constitution provides for tha the Fifth Amendment. But the salaries of governm workers are still paid by the people, and the gove ment has an obligation to confront the people v the facts about how their government is run, es cially in peacetime. If we have gone so far in t country that we do not understand that, then we over the hill.

HALPERIN: Has the C.I.A. been acting like a ro elephant off on its own or, as Mr. Cline tells us, it always obeyed the orders of the President? It wo be remarkable if indeed the C.I.A. had always obe orders and never lied to its superiors. It would be only such institution in the history of the world. the other hand, the record suggests that the C.I has not been going off in large measure and ignor the orders of its Presidents. Most of the things C.I.A. has done and that the F.B.I. has done things our Presidents wanted them to do. Nob can read the description of the Lumumba assassi tion in Senator Church's committee report with thinking that President Eisenhower, if he didn't w to know that Lumumba was going to be assassina certainly wanted him out of the picture and not care how it was done. Nor is there any do in my mind that Lyndon Johnson wanted C.I.A. to find out as much about the nineteen-sixt

antiwar movement in the United States as it could.

One does have to say that there have been cases in which the C.I.A., like all other agencies, deliberately disobeyed the President or failed to consult with him when it knew it was doing something wrong. The difference is that when the C.I.A. does this, it can have very substantial consequences. We now know that the C.I.A. opened thousands of letters of citizens going to and from many different countries over a twenty-year period. It knew it was illegal to do that, but it never got around to telling the President that this was going on.

It is also clear from Senator Church's committee report that when Lyndon Johnson wanted to be sure that our government was not trying to assassinate Castro and to find out whether we had previously tried to assassinate Castro, he got a report from Richard Helms which did not tell him of the view of the Inspector General of the C.I.A. that we were then conducting an operation which was an assassination attempt. President Johnson was left with the view that if that had gone on in the past, it had now been stopped.

So, while it is not true that the C.I.A. is totally out of control, it is true that we cannot count on it always to obey the law or the directives of the President.

CHURCH: I want to compliment Mr. Halperin for his statement. It puts this whole thing into perspective.

STEWART MOTT *(Center and Fund for Peace Director):* Should the law of the country allow the C.I.A. or its operatives knowingly to break the criminal code of the United States or any foreign country?

COLBY: I would say certainly not of the United States. But most countries have laws against espionage, and it would be very difficult, indeed, to conduct our intelligence operations without breaking a few of those.

CLINE: I think there is a misunderstanding about covert operations. People believe that it means organizing armies and conducting vast illegal campaigns. The most successful covert intelligence operations are those in which no law is broken and in which the U.S. point of view and, in many cases, its financial assistance, are given to constructive elements in foreign countries. As far as I know, that does not break any foreign law.

If we want to fight against Cuba or the Congo or Vietnam, or whomever, we ought to have the guts to say it is a war and fight with all the means we have. We ought not to give the job to the C.I.A. in the hope that it can be done quietly and secretly without anybody noticing it.

HALPERIN: Mr. Cline chooses to tell us what we always hear — that our great success was the support we gave to democratic forces in Europe in 1948. The kind of covert operation I am objecting to is the kind that led the American government to go to the military of Chile and say to them, "You may think you are going to continue your constitutional processes; and you may think it is all right for your parliament to meet and lawfully elect Mr. Allende. But that is unacceptable to the United States. So, if you go ahead with your democratic process, we will do everything we can to starve the people of Chile. What we suggest you do is kidnap the Chief of Staff of your army because he is in favor of your constitution. And then have a military coup and overthrow the government so that Mr. Allende will not come to power."

That is the kind of covert operation I object to, and I submit that that is the kind of covert operation the C.I.A. in fact has been conducting in very many countries throughout the world.

CLINE: That is the kind of covert operation I do not support either. The covert operation in Chile in 1970 and 1971 was laid on by President Nixon and Henry Kissinger without very much consultation with the intelligence community. I know, because I was Director of Intelligence in the State Department at the time. Many intelligence people regretted that operation.

The kind of covert operation I support is the financial assistance and informational assistance given to newspapers and to public opinion media in Chile in 1963 and 1964 to support the Christian Democratic efforts of Eduardo Frei, who was undoubtedly the most popular man in Chile. If Frei had not been ineligible for re-election I am sure that Allende would never have been elected. The C.I.A.'s program was to try to create a moderate center parliamentary government in Chile with a progressive social and economic program. It did pretty well for several years. That program was discontinued in the late nineteen-sixties. And then what I consider to have been a misbegotten, belated attempt to do something in Chile was laid on by the White House.

COLBY: With one exception, which was directed

personally by the President of the United States, the C.I.A.'s program in Chile over many years was essentially one of supporting democratic forces. That started many years ago and, in answer to Mr. Halperin's question — "When did you last support liberal democratic forces in a country?" — it terminated in 1973. Our effort during that period was to sustain democratic forces, parties, groups, media at a time when they were being pressured and suppressed by a government which represented thirty-six per cent of the voters. That government was denounced by the Chilean Congress, by its Supreme Court, and by its comptroller general as operating outside the constitution.

Now, we made a conscious decision — with that one exception in 1970 — that we did not want to bring about a military coup. We separated ourselves from the leaders of the military who did lead the coup. Our policy was to look forward to the elections of 1976 which we hoped the democratic forces in Chile would win. We had nothing to do with the overthrow by the army which we had always appraised as being perhaps one of the most constitutional armies in Latin America. But the army was driven to the wall in the summer of 1973 and, on their own, as they have testified themselves, and as I think our evidence indicates, they carried out the coup that overthrew Mr. Allende.

There has been a total misconception of the C.I.A.'s program and policy in Chile, stemming from some misinterpretations of testimony I gave in 1973 to an executive session of our congressional oversight committee. Words were put into my mouth characterizing our program in Chile as one of "destabilization." I never used that word, and I did not think that that was what our program was. It was rather one of supporting the democratic forces during a period in which they were under a great deal of pressure.

CHURCH: It is, of course, true that Mr. Allende was elected by a plurality, not a majority, of the vote. It is also true that Richard Nixon was elected by a plurality of the vote, not a majority. Both were legitimate Presidents under the constitutions of their respective countries. In every case in the previous history of Chile, when a candidate got a plurality of the vote, he was the candidate then chosen to be President by the Congress as having received the largest number of votes.

It is also true that Mr. Allende's government — for which I hold no brief, I thought it was a dreadful government — moved to curtail freedom in Chile but not so far as to declare opposition parties unlawful. Those continued to function. The basic institutions of government continued to function. There were municipal elections. People continued to vote. And compare the amount of democracy that still lived under Allende, who did believe in the constitutional system, to what there was in the terrible bloodbath that brought on the present fascist government after Allende.

The one exception noted by Mr. Colby was a mighty big exception: it was to overthrow Allende, by a military *coup d'état*, after he had been elected. So everything we did was wrong. Even though we did not have a hand in the final overthrow of the Allende regime, our participation in the effort to destroy that regime from the outset inevitably led to the uprising and to the bloodbath and the kind of regime that followed it.

Now all over South America our capacity to exert moral leadership and the belief in the United States has been drastically weakened. That is the problem with this covert business. The President of the United States is not Caesar, and the western hemisphere is not a colony of the United States. Washington has no right to intervene and decide for other people what kind of government they shall have. We once knew that. We once practiced it. Those were the days when we were the most respected country in the world.

MORGAN: Mr. Cline says no law is broken when foreigners spend money in other countries. Well, I suppose we support that every day in every Chamber of Commerce, except that he is talking about something else. We see on the front pages stories about oil companies spending tens of millions of dollars corrupting, bribing foreign governments, working with our C.I.A. And we are told that the statute of limitations expired on the Ashland Oil Company. That was what the Watergate special prosecutor said about the contribution made to the Democratic Party by Ashland Oil. A month later a funny thing came out about Ashland Oil; it was that it had a slush fund for overseas political payments. Then another funny thing came out a couple of weeks later, that the C.I.A. had money in it.

And who was corrupted when Howard Hughes' lawyers went to the tax assessors and told them not to include that secret ship? Who was corrupted when a decent public official said "national security" on that? And who was corrupted when a fake certificate of ownership on that ship was given to the Coast Guard?

We do have a moral responsibility to try to support those kinds of societies that Senator Church spoke about. — RAY S. CLINE

That was a lie and a perjury. Who was corrupted when the Securities and Exchange Commission did not come forward and enforce the laws on Hughes? What does that do to the lawyers in that governmental agency? What does it do when you do not extradite, when the Justice Department says don't go after Howard Hughes, don't bring him in?

It means that we have corrupted ourselves as far as these kinds of covert activities are concerned, Mr. Cline.

MOTT: I think all of us here would find it rather obnoxious if it were learned that the American Independent Party, or George Wallace, or Ronald Reagan were being supported by some foreign fascist regime. It would be equally obnoxious if we learned that the campaigns of Eugene McCarthy or George McGovern were financed by the Soviet Union. We have laws against that. We respect the integrity of the political process at home. Then how can we condone the notion that we do not need to respect the same process in other countries? How can we justify our intervening with advice and money, overtly or covertly? I know the answer is not simple. The French did help us during the American Revolution to get where we are today.

CHURCH: That is the hardest question that has been asked today. On principle, there is no way one can defend a covert undertaking by the United States to finance a political party or a political movement in a foreign country.

But there is another element in the picture, the very persistent and aggressive Soviet Union which, I suppose, is less troubled by such moral questions than we are. The Soviet Union has intervened very actively and has contributed a good deal of money and other kinds of help on behalf of political movements — namely, Communist movements — within other countries. And it is only in those situations — say in a little country like Portugal, in which the Soviet Union has decided it will try to turn it Communist by a massive covert penetration and by forcibly imposing a minority party on eighty-four per cent of the Portuguese people — that you have got to say it is permissible for the United States to step in and try to give a hand to the large majority of Portuguese who are trying to achieve and preserve a free government.

MOTT: The great difficulty is that for years and years now that is not what we have been doing in our covert operations. We have been doing just the opposite. We have thought it was our mission to be the sentinel of the status quo in a world that is largely in ferment and largely controlled by despotic, repressive, rotten governments of one kind or another. Our covert actions seem to have been designed to keep those governments in place, as though we could squelch all the volcanoes of revolution. That has put us on the wrong side. Our covert actions have been completely contrary to our traditional principles, and have undermined the prestige, good name, and reputation of the United States throughout the world.

CLINE: Suppose that in a country like Portugal it was absolutely clear that thirteen per cent of the people were about to establish, through military force and propaganda operations, a one-party dictatorship under Soviet or some other totalitarian society's control. Would you walk away from that problem? Many of the comments here have suggested yes, we should walk away. That is what I call the "Kitty Genovese" complex. We do have a moral responsibility to try to support those kinds of societies that Senator Church spoke about. Maybe we have not supported all the right ones; that is a policy decision. But we ought to support them.

MORGAN: What country have we supported over the

years which is not headed by a petty dictator of one sort or another? Today, after overthrowing Allende and, before that, killing General Schneider, we are getting ready to recognize Cuba — a dictatorship — and the President of the United States and Henry Kissinger are over in China toasting. . . . I say, is peace so dear, or is it democracy that we are talking about? Have we come so far that this kind of conduct and covert activity are part of our lives and ways? If they are, I choose to secede from that, and I trust most citizens will also when they are confronted with it.

And what is all this talk about the "real world" and the fact that the Russians are doing this or that? We can't live by their standards. Machiavellianism does not apply in a democracy. That is the one place it does not apply. We cannot live by the lie. The ideal is the real. All we have to do is to live by our own documents, and the world will be in revolution to have what we have.

COLBY: The framework of covert action has always been the interests of the United States as a sovereign power in a world in which there are other sovereign powers. We have not been on an ideological crusade, and that explains why we have responded to threats by another great power and its local satraps and why we have not conducted an ideological crusade to overthrow right-wing governments around the world. Right-wing governments have not constituted a threat to the United States. If they do, presumably we will do something about that problem.

MORGAN: But that thinking constitutes a threat to democracy, and that is a threat to the United States.

COLBY: I think that will be resolved by the Congress. Covert actions will be undertaken only with the knowledge of a representative committee in the Congress. When we should do it and when we should not do it will be determined according to the representative government and the constitutional structure of our country

HALPERIN: Mr. Colby has just made clear why it is no accident that the United States has not intervened on the side of democratic forces. We have only been interested in our own national interest, as we define it. That means that a Portuguese government which, for twenty-five years, has been a repressive totalitarian regime was totally acceptable to the United States. It gave us the military bases we wanted; it cooperated with us in our military security. We are concerned about Portugal now because we fear that a government will come to power which will not give us those bases, which will not cooperate with us in defining security as we define it. Inevitably that means that the United States ends up supporting safe regimes which are right-wing military dictatorships because left-wing governments threaten to become antagonistic to us or friendly to the Soviet Union.

If we are going to intervene, consistent with our ideals, we can do it openly. It is no secret to anybody that we are intervening now in Portugal. It is no secret that Western European democratic parties are intervening in Portugal, or that Communist parties are intervening in Portugal. There is no reason why U.S. intervention cannot be a publicly argued decision in this country, no reason why the President cannot ask for funds for this, as he does for other purposes. Then we can debate whether we want to give that kind of aid to these people. Where something like that is consistent with our interest and our ideals, we can do it openly. We have to do it covertly only when the President knows he cannot get the support of the people or the Congress because it is contrary to Congress' view of our interests or our ideals.

CHURCH: I very much agree with what Mr. Halperin has just said. In pursuing our interest through normal diplomatic channels, we must accept governments as they come — the dictatorships, the democracies, the despotisms, the Communist states — we have to accept them and deal with them as best we can. We can protect our strategic interests with open alliances, even though in some cases those may be with governments we do not approve.

But when it comes to covert actions to manipulate events within foreign countries, then I am afraid that in the last twenty years we have been far more controlled by our fears than by faith in our own system. Our fear has been that revolution in itself threatens us because the Communists somehow will emerge and control the world, and that we will slowly sink in a great red sea.

Now it is that cold war fantasy, that obsession, that we must throw aside. Five thousand years of history have taught us that this world is too big, that people are too tough, that the philosophies of various religions and cultures are too diverse for any one nation to be able to control it all. Let us get back to faith in our own system and never intervene on any other basis than that. ☆

[Harvard Law Review, v. 85, April 1972]

THE NATIONAL SECURITY INTEREST AND CIVIL LIBERTIES

Those who would give up essential Liberty, to purchase a little temporar Safety, deserve neither Liberty nor Safety.

LETTER OF PENNSYLVANIA ASSEMBLY TO GOVERNOR ROBERT MORRIS, NOV. 11, 1755

TABLE OF CONTENTS

PAGE

I. INTRODUCTION 11

II. EXAGGERATED FEARS FOR THE NATIONAL SECURITY: SOME EXPERIENCE TO DATE 11

A. Criminal Punishment of Speech and Association 11

1. Advocacy and Group Membership 11

2. Symbolic Speech 11

B. Restrictions on International Travel 11

1. Area Restrictions 11

(a) The Government Interests 11

(b) The Civil Liberties Interests 11

(c) An Evaluation of Area Restrictions 11

2. Restrictions on the Foreign Travel of American Subversives 11

3. Restrictions on Entry of Alien Subversives into the United States 11

C. Loyalty Tests for Employment 11

1. Present Loyalty and Security Programs 11

(a) State Loyalty Tests 11

(b) Federal Programs 11

(c) Outline for an Evaluation 11

2. Substantive Criteria for Loyalty Dismissals 11

(a) Judicially Imposed Restraints 11

(b) Evaluation of the Judicial Approach 11

3. Means of Obtaining Information to Administer Loyalty Programs 11

(a) Self-executing Screening Programs 11

(b) Administrative Loyalty Programs 11

(i) Compulsory Disclosure Requirements 11

(ii) Investigations 11

(iii) Due Process Protections 11

4. Conclusion 11

III. INFORMATION SECURITY: CLASSIFICATION OF GOVERNMENT DOCUMENTS 11

A. Classification of Sensitive Information 11

1. The Necessity for Official Secrecy 11

2. The Historical Background 11

3. The Classification System 11

(a) Statutory and Constitutional Authority 11

(b) Executive Order 10,501 11

(i) Classification Criteria and Procedures 11

(ii) Declassification 12

(c) Executive Order 11,652 12

79-064 O - 76 - 41

PAGE

4. The Disclosure of Classified Information 1205
B. Executive Withholding of Information from Congress 1207
1. Effect of the Classification System on the Availability of Information to Congress 1208
2. Executive Refusals to Comply with Congressional Demands for Information: The Executive Privilege 1212
C. External Checks on Executive Secrecy 1215
1. Constitutional Bars to Judicial and Legislative Checks 1217
2. Judicial Checks on Executive Secrecy: The Freedom of Information Act 1221
3. Proposals for Legislative Action 1227
(a) Controlling Classification 1227
(i) Evaluation of Executive Order 11,652 1227
(ii) Legislative Proposals 1229
(b) Increasing the Flow of Information to Congress 1231
D. Enforcement of Secrecy 1232
1. The Espionage Laws 1232
(a) Espionage Activities 1232
(b) Public Disclosures 1233
2. First Amendment Considerations 1239
(a) Sanctions on the Press 1239
(b) Sanctions on Government Employees 1243

COVERT GOVERNMENT SURVEILLANCE 1244
A. Electronic Surveillance 1246
1. A Brief History of the Legal Status of National Security Electronic Surveillance 1248
2. The Extent of Inherent Presidential Authority 1257
(a) The Duty as Commander in Chief 1257
(i) In the Absence of Hostilities at the Place of Surveillance 1257
(ii) With Hostilities Proximate to the Place of Surveillance 1258
(iii) Conclusion 1259
(b) The Duty to Maintain the Rule of Law at Home 1259
(c) The Duty to Conduct Foreign Affairs 1260
(d) The Inherent Power to Conduct Electronic Surveillance of Foreign Government Officials in the United States 1261
3. The Reasonableness of Warrantless National Security Electronic Surveillance Under the Fourth Amendment 1262
(a) The First Exception: Camara *and* James 1263
(b) The Second Exception: Terry v. Ohio 1264
(c) The Inapplicability of the Two Exceptions: First Amendment Considerations 1264
(d) The Reasonableness of Electronic Eavesdropping on Foreign Government Officials in the United States 1266
4. Some Special Considerations Attending Authorization of Electronic Surveillance by the Attorney General 1268
B. Informers 1270
1. First Amendment Interests Affected 1274
2. Control of Informers 1277

THE EXERCISE OF EMERGENCY POWERS 1284
A. Introduction 1284
B. Checks on the Use of Emergency Powers 1287
1. General Guidelines 1287
2. Legislative Participation in the Exercise of Emergency Powers 1288
3. Judicial Review of the Use of Emergency Measures 1293
(a) The Traditional Standards of Review 1294

* * * * * * *

IV. Covert Government Surveillance

In no area has experience more clearly indicated the executive branch's tendency to overrate threats to the national security than with regard to dissident domestic political organizations. Indeed, the stark examples we met earlier of such exaggerated fears — flag desecration statutes,[1] restrictions on contact with foreigners,[2] and employment security standards only tenuously related to real job demands [3] — were all engendered by domestic political dissent.

To the degree that a political organization genuinely threatens

[1] *See* Section II.A. *supra*.
[2] *See* Section II.B. *supra*.
[3] *See* Section II.C. *supra*.

the national security, it is the duty of the executive to keep itself informed of that organization's activities and plans. Even in such a case, however, guarantees of privacy afforded the organization's members by the fourth amendment may restrict the methods of intelligence collection legitimately available. Equally important, the danger that the executive will perceive security threats where there are none may call for articulation and enforcement of restrictive standards for domestic intelligence collection under the first amendment — to reduce the potential for government inhibition of protected political activity.

This section will be concerned with two intelligence techniques — the use of warrantless electronic surveillance and the deployment of Government-directed informers — which are closely associated with security investigations. Although both techniques are used for the clandestine gathering of investigative information, the issues and even the forum for dispute differ markedly between the two collection methods.

The Supreme Court has declared the fourth amendment applicable to electronic surveillance.[4] The Court's requirement of disclosure of the transcripts of all illegal electronic surveillance to any criminal defendant who has been thus overheard [5] has given leverage to the federal judiciary to control government eavesdropping. While the Court has not yet decided whether national security electronic surveillance is, like all other government electronic eavesdropping, subject to the requirements of judicial warrant and probable cause, that leverage will better enable the courts to enforce such a holding if it is announced. Such judicial enforcement could be a most effective mode of controlling electronic surveillance of both domestic dissidents and foreign officials within the United States.[6]

The case with Government-directed informers is quite different. There the Court has refused to apply the fourth amendment requirements of prior judicial authorization and probable cause even outside the national security context.[7] Therefore, any comprehensive constitutional restraint on the use of informers within the national security area must rest on the first amendment — on the danger that informers will infiltrate and thereby perhaps inhibit protected political activity. Unlike the fourth amendment, however, the first amendment makes no explicit provision for prior judicial authorization of government practices. Even if it did so, the use of informers, in contrast to

[4] Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967).

[5] Alderman v. United States, 394 U.S. 165 (1969).

[6] *See* p. 1269 *infra*.

[7] Hoffa v. United States, 385 U.S. 293 (1966).

national security electronic surveillance, is a somewhat informal, large-scale activity, traditionally engaged in at low levels of the law enforcement bureaucracy, and often resulting in no identifiable government action against a citizen. The imposition of effective judicial sanctions against the misuse of informers could be extremely difficult.[8] Therefore, the argument as to the effective control of informers must be directed at least as much to the executive branch as to the courts.

A. Electronic Surveillance

The Nixon Administration claims that the executive branch has almost absolute constitutional authority to employ wiretapping and electronic "bugs" to protect the national security. In the investigation of crimes unrelated to the national security, electronic surveillance is authorized by statute[9] and permitted by the Constitution[10] only when a judicial officer issues a warrant indicating that there is probable cause to believe evidence of a crime will be obtained.[11] But in briefs recently submitted to the Supreme Court, the Administration, arguably with statutory support,[12] contends that a set of safeguards less stringent than a judicial warrant based on probable cause is constitutionally adequate to justify national security surveillance.

The proposed safeguards would consist of, first, prior approval of national security taps and bugs by the Attorney General of the United States, acting as the President's delegate,[13] and second, authorization of such surveillance in the domestic area only when necessary "to protect the United States against the overthrow of the Government by force or other unlawful means or against any other clear and present danger to the structure or existence of the Government."[14] While this standard is con

---

[8] *See* pp. 1280–81 *infra*.

[9] Omnibus Crime Control and Safe Streets Act of 1968, tit. III, § 802, 18 U.S.C. §§ 2516–18 (1970).

[10] Katz v. United States, 389 U.S. 347 (1967) (warrantless, nontrespasser bugging of telephone booth held to be violation of fourth amendment).

[11] Before issuing an order authorizing electronic surveillance, the judicial officer by statutory requirement must find not only that probable cause exists but as well that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(3)(c) (1970).

[12] *See* p. 1260 *infra*.

[13] Brief for Petitioner at 19, United States v. United States Dist. Court, 444 F.2d 651 (6th Cir.), *cert. granted*, 403 U.S. 930 (1971) (No. 1687) [hereinafter cited as Government Brief].

[14] *Id.* at 20–21. This is the same standard under which domestic security electronic surveillance is exempted from the statutory warrant requirements of 18 U.S.C. §§ 2516–18 (1970). 18 U.S.C. § 2511(3) (1970). *See also* p. 1136 *supra*.

ceded by the Government to be reviewable in court in the event a tap or bug is at issue in criminal proceedings,[15] the proposed review is to be far narrower than the de novo scrutiny ordinarily given to a warrant at a suppression hearing prior to a criminal trial.[16] National security taps, it is said, should be disapproved only if they constitute a "clear abuse" of the broad discretion that the Attorney General has to obtain all the information that will be helpful to the President in protecting the Government against "overthrow."[17] The Government has not clearly indicated what activities it is sure would fall outside the national security category. The determination of the bounds of the category is left, instead, in very large measure, to the discretion of the Attorney General.

Pursuant to this asserted authority, the federal government has engaged in what it claims to be a limited program of national security electronic surveillance. In March 1971 congressional testimony, FBI Director J. Edgar Hoover reported that the FBI was conducting thirty-three wiretaps *at that time* in "Bureau cases in the security field."[18] However, because this figure may not include the FBI's use of local law enforcement agency taps, the FBI's conduct of national security taps for agencies such as the CIA in non-Bureau cases, and FBI agents' conduct of security taps without official Bureau authorization, it has been suggested that the Director's statement may underestimate the number of government national security taps.[19] Giving some idea of the scope of the conduct of warrantless national security electronic surveillance over a longer time span is an exchange of letters between Assistant Attorney General Robert Mardian and Senator Edward Kennedy.[20] In them, Mardian indicated that during 1970, ninety-seven warrantless national security wiretaps and sixteen warrantless national security microphone surveillances were conducted.[21]

---

[15] Government Brief 21. The Government would provide for no judicial review at all of national security taps where no criminal proceedings are brought.

[16] *See, e.g.*, Aguilar v. Texas, 378 U.S. 108 (1964).

[17] Government Brief 22.

[18] *Hearings on Dep'ts of State, Justice, and Commerce, the Judiciary, and Related Agencies Appropriations for 1972 Before a Subcomm. of the House Comm. on Appropriations*, 92d Cong., 1st Sess., pt. 1, at 752 (1971).

[19] N. Lewin & V. Navasky, The FBI and Electronic Surveillance 54–56g, Oct. 29, 1971 (unpublished paper delivered at conference on the FBI sponsored by the Committee for Public Justice; on file at the *Harvard Law Review*).

[20] Taking place between Feb. 5, 1971, and Apr. 23, 1971, the exchange is reprinted in Brief for ACLU as Amicus Curiae at 51–66, United States v. United States Dist. Court, 444 F.2d 651 (6th Cir.), *cert. granted*, 403 U.S. 930 (1971) (No. 1687) [hereinafter cited as ACLU Brief].

[21] Letter from Assistant Attorney General Robert Mardian to Senator Edward Kennedy, March 1, 1971, in ACLU Brief 57–60.

The debate whether national security electronic surveillance is constitutional without a warrant and probable cause assumes operational significance when the defendant in a criminal trial suspects the Government of attempting to introduce evidence obtained by electronic spying — or its fruits.[22] Any evidence obtained in violation of a defendant's fourth amendment rights is inadmissible in both federal[23] and state[24] tribunals. The entire dispute about the constitutionality of national security surveillance without a warrant or probable cause centers on the admissibility of evidence.

As a result, the dispute received little attention until the Supreme Court's 1967 decisions in *Katz v. United States*[25] and *Berger v. New York*,[26] which indicated for the first time that electronic surveillance constituted a search and seizure, and that its fruits were therefore subject to exclusion if fourth amendment probable cause and warrant requirements were not satisfied. The full extent to which *Katz* and *Berger* might offend the political branches if applied in national security cases[27] became apparent just one year later, when Congress passed legislation apparently intended to remove all statutory obstacles to executive-controlled electronic surveillance in the national security field.[28] The constitutionality of that legislation, and the viability of the Nixon Administration's present argument before the Supreme Court, are best evaluated after a brief historical review.

1. A Brief History of the Legal Status of National Security Electronic Surveillance. — Since long before *Katz* or *Berger*, federal courts have refused to receive evidence obtained by electronic surveillance. The exclusion of wiretap evidence, however, was based on statutory rather than constitutional exegesis — and the 1968 Omnibus Crime Control Act effectively repealed the

---

[22] *See* pp. 1253–55 *infra*.

[23] Weeks v. United States, 232 U.S. 383 (1914).

[24] Mapp v. Ohio, 367 U.S. 643 (1961).

[25] 389 U.S. 347 (1967).

[26] 388 U.S. 41 (1967) (New York system of court ordered electronic surveillance held not to satisfy fourth amendment).

[27] The Court in *Katz* explicitly limited its ruling to the treatment of non-national security electronic surveillance. "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." 389 U.S. at 358 n.23. In concurrence, Justice White argued that there should be no warrant requirement for national security wiretapping. *Id.* at 363–64. Justice Douglas, joined by Justice Brennan, wrote a concurring opinion in which he differed with White: "[S]pies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers . . . ." *Id.* at 360.

[28] Omnibus Crime Control and Safe Streets Act of 1968, tit. III, § 802, 18 U.S.C. § 2511(3) (1970). *See* p. 1252 *infra*.

underlying statute in the national security field. What is more, while the exclusion of evidence obtained by almost all bugging had been constitutionally impelled from the outset, its original constitutional foundation — that bugging could be unlawful only if there was physical trespass — had been eroded by technological "progress." For either type of electronic surveillance, therefore, any remaining exclusionary rule in national security cases must be derived from *Katz* or *Berger*.

The longstanding refusal of federal courts to exclude wiretap evidence on constitutional grounds derived from the 1928 case of *Olmstead v. United States*.[29] There the Supreme Court held that wiretapping was not a search and seizure and could not violate the fourth amendment, because it did not involve entry into the victim's home or office and because the spoken word could not be "seized." The trespass doctrine of *Olmstead* was subsequently applied in bugging cases,[30] while the "word seizure" doctrine seemed to drop away.[31] Since bugging, as distinguished from wiretapping, was for a long time technologically very difficult without at least a minimal physical intrusion on the victime's premises, most bugged evidence, unlike wiretap evidence, was constitutionally excluded.[32]

The statutory foundation for exclusion of wiretap evidence was the Federal Communications Act of 1934. The Act established criminal penalties for anyone who engaged in the "interception and divulgence" of wire communications.[33] Since testifying to the contents of a tap was held to constitute divulgence within the meaning of the statute, the Supreme Court barred federal judges from receiving such testimony.[34] The Court also ruled against admissibility of evidence derived from wiretapping to

---

[29] 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

[30] Silverman v. United States, 365 U.S. 505 (1961) (trespass); Goldman v. United States, 316 U.S. 129 (1942) (no trespass).

[31] *See* Silverman v. United States, 365 U.S. 505 (1961); Goldman v. United States, 316 U.S. 129 (1942).

[32] *See* Silverman v. United States, 365 U.S. 505 (1961). *But see* Goldman v. United States, 316 U.S. 129 (1942).

[33] Federal Communications Act of 1934 § 605, ch. 652, § 605, 48 Stat. 1103 (1934), *as amended* 47 U.S.C. § 605 (1970). Although there is some question as to whether § 605 was meant to apply to telephone communications, *see* J. LANDYNSKI, SEARCH AND SEIZURE IN THE SUPREME COURT 206 (1966), the Supreme Court from the outset determined that the regulation of wiretapping was within the plain mandate of the statute. Nardone v. United States, 302 U.S. 379, 383 (1937).

[34] Nardone v. United States, 302 U.S. 379 (1937). The Supreme Court rejected the Government's contention that § 605 did not apply to government law enforcement agencies.

ensure that the legislative policy against wiretapping was not frustrated.[35]

Although the statutory basis for the wiretap exclusionary rule remained effective until 1968,[36] the executive wiretapped in the national security field throughout most of that period — and simply avoided any apparent use of wiretap evidence in federal court. Attorney General Jackson's initial reaction to the Supreme Court's wiretap exclusionary rule was to announce in early 1940 that wiretapping would no longer be employed by the Government.[37] But just two months later President Roosevelt proclaimed his view that the statutory ban was inapplicable "to grave matters involving the defense of the nation."[38] The President felt compelled by the "fifth column danger" posed by Nazis and their sympathizers to authorize Jackson to approve taps of "persons suspected of subversive activities against the Government of the United States, including suspected spies."[39]

Although the Roosevelt directive contained two safeguards designed to minimize the infringement of American citizens' constitutional rights, those restraints were eventually eroded. First, Roosevelt instructed Jackson to oversee each tap personally.[40] But the Attorney General delegated his responsibility to the Director of the FBI.[41] Second, Jackson's charter was

---

[35] Nardone v. United States, 308 U.S. 338, 340 (1939). The Court felt that even indirect use of the taps in a federal prosecution would violate the ethical standards which § 605 was attempting to promote. Although the reach of *Nardone*'s exclusionary rule was originally thought to extend only to evidence presented in federal court, Schwartz v. Texas, 344 U.S. 199 (1952) (wiretap evidence admitted in state trial), this limitation was eventually discarded so that even wiretap evidence offered in state courts by state officials was held inadmissible. Lee v. Florida, 392 U.S. 378 (1968).

[36] Attempts to obtain explicit congressional authorization for national security wiretapping, even during the Second World War, were unsuccessful. For example, legislation to allow the executive branch to conduct wiretapping in the interest of the prosecution of the War, H.R.J. Res. 310, 77th Cong., 2d Sess. (1942), was reported on favorably by the House Committee on the Judiciary, H.R. Rep. No. 2079, 77th Cong., 2d Sess. (1942), and passed by the full House. 88 Cong. Rec. 4602 (1942). It was, however, never enacted by the Senate. *See* Gasque, *Wiretapping: A History of Federal Legislation and Supreme Court Decisions*, 15 S.C.L. Rev. 593, 601 (1963).

[37] Press Statement of the Department of Justice, released March 18, 1940, dated March 15, 1940. *See* Brownell, *The Public Security and Wire Tapping*, 39 Cornell L.Q. 195, 199 & n.16 (1954).

[38] Memorandum from President Roosevelt to Attorney General Jackson, May 21, 1940, printed in United States v. United States Dist. Court, 444 F.2d 651, 669–70 (6th Cir.), *cert. granted*, 403 U.S. 930 (1971) (No. 1687) [hereinafter cited as Roosevelt Memorandum].

[39] Roosevelt Memorandum 670.

[40] *Id.*

[41] Francis Biddle, Solicitor General at the time, recalled that Jackson "turned

qualified by a directive to "limit [the taps], insofar as possible to aliens." [42] Indeed, the tone of the memorandum suggests Roosevelt was sensitive to civil liberties dangers from the abuse of wiretapping, and therefore conceived his memorandum as strictly a wartime measure, inapplicable to wholly domestic political organizations.[43] But this second restraint fell away with the onset of the Cold War.

After the close of World War II, Attorney General Clark obtained President Truman's agreement to a memorandum [44] affirming the 1940 directive as to "subversive activities" even in peacetime and omitting the prior directive's request to limit taps to aliens. The new document asserted that taps were imperative in "cases vitally affecting the domestic security." [45] Indeed, it extended wiretap authority still further, to ordinary criminal cases "where human life is in jeopardy." [46] On the foundation of Truman's (and Roosevelt's) directive, Government wiretapping continued throughout the 1950's and 1960's.[47]

So long as the statutory base of the wiretap exclusionary rule remained firm, attempts to introduce wiretap-based evidence in court consistently failed, even in espionage cases involving Soviet agents.[48] Thus, eavesdropping under the "security" justification of the Truman memorandum could be used only as an intelligence gathering device rather than as a prosecution-related tool. But as the Cold War continued, Congress' commitment to the philosophy of the Federal Communications Act provisions seemed to wane. Executive use of wiretapping aroused little

---

[the memorandum] over to Edgar Hoover without himself passing on each case." The quotation appears in V. NAVASKY, KENNEDY JUSTICE 73 (1971).

[42] Roosevelt Memorandum 670.

[43] "[U]nder . . . normal circumstances wire-tapping by Government agents should not be carried on for the excellent reason that it is almost bound to lead to abuse of civil rights." *Id.* at 669; *see* Comment, *Privacy and Political Freedom: Application of the Fourth Amendment to "National Security" Investigations*, 17 U.C.L.A.L. REV. 1205, 1222 (1970).

[44] Memorandum from Attorney General Clark to President Truman, July 17, 1946(or 1947), printed in United States v. United States Dist. Court, 444 F.2d 651, 670 (6th Cir.), *cert. granted*, 403 U.S. 930 (1971) (No. 1687).

[45] *Id.*

[46] *Id.*

[47] In 1950 FBI Director Hoover, relying on the presidential memoranda for authorization, testified that the FBI had "less than 170 telephone taps." *Hearings on Dep't of Justice Appropriation for 1951 Before Subcomm. of the House Comm. on Appropriations*, 81st Cong., 2d Sess., at 230 (1950). *See also* p. 1247 *supra*.

[48] In the espionage case of United States v. Coplon, 88 F. Supp. 921 (S.D.N.Y.), Judge Ryan observed that the memoranda did not "detract at all from the interdiction of the Supreme Court on evidence secured by this type of investigation." *Id.* at 925.

public opposition.[49] Indeed, when the executive more forthrightly acknowledged the extent of its use of wiretapping [50] during the Red Scare of the 1950's, congressional hearings were held [51] *not* with intent to limit wiretapping, but to discuss statutory reversal of the wiretap exclusionary rule.[52]

Congressional unease with the wiretap exclusionary rule climaxed in passage of the Omnibus Crime Control and Safe Streets Act of 1968. Wiretapping, along with bugging, had come to be seen as an indispensable evidence gathering device, particularly in the struggle against organized crime.[53] Of more direct concern here, some legislators felt both practices would be of special utility in preventing incidents of sabotage and mass violence allegedly directed by dissident political groups.[54] The legislation authorized wiretapping and eavesdropping by law enforcement officials. For cases involving non-national security crimes, judicial warrants based on probable cause were required [55] — in accordance with traditional fourth amendment practice and the *Katz* and *Berger* decisions of the previous year.[56] The traditional standards were abandoned, however, in situations involving the collection of intelligence both for diplomatic and defense planning, and for the protection of national security against domestic subversion. In such cases, Congress removed all statutory obstacles both to the conduct of national security electronic surveillance and to the introduction of evidence gleaned from such taps and bugs as long as the interception was "reasonable." [57]

---

[49] A. WESTIN, PRIVACY AND FREEDOM 174 (1967).

[50] The confidential presidential memoranda of the 1940's were supplemented in the 1950's by vigorous administration advocacy of legalized wiretapping. *See* Brownell, *supra* note 37; Rogers, *The Case for Wire Tapping*, 63 YALE L.J. 792 (1954).

[51] *E.g.*, *Hearings on Wiretapping for National Security Before Subcomm. No. 3 of the House Comm. on the Judiciary*, 83d Cong., 1st Sess. (1953).

[52] *Id.* at 16–17. *See* Theoharis & Meyer, *The "National Security" Justification for Electronic Eavesdropping: An Elusive Exception*, 14 WAYNE L. REV. 749, 764 (1968).

[53] S. REP. No. 1097, 90th Cong., 2d Sess. 70 (1968).

[54] Senator McClellan, a notable advocate of electronic surveillance legislation, felt that any legislation to be enacted should enable the Government to "bug a room or a hall in which Carmichael was meeting, in which Rap Brown was meeting, where they were inciting to riot, telling people to get their guns, 'Go get whitey,' and do this and do that." 114 CONG. REC. 14,702–03 (1968).

[55] 18 U.S.C. § 2518(3) (1970).

[56] *See* p. 1248 *supra*.

[57]

> Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential

If any exclusionary rule remained with regard to wiret and bug-related evidence in national security cases, it had to be constitutionally based. Also, since it had become feasible to bug, as it always had been to tap, without a trespassory intrusion,[58] any constitutional exclusion of evidence derived from national security electronic surveillance had to rest on the cases reversing *Olmstead*.

But while *Katz* and *Berger* had brought electronic surveillance within the fourth amendment, requiring judicial warrants and probable cause, *Katz* had explicitly reserved the applicability of its holding in national security cases.[59] In 1969, Attorney General Mitchell attempted to answer the reserved question with regard to domestic national security electronic surveillance, flatly asserting the executive's constitutional power to sidestep the warrant procedure when national security is threatened.[60] But no national security case decided by the Supreme Court after *Katz* has dealt directly with the propriety of introducing evidence based on warrantless national security taps.

In the meantime, the Supreme Court decision in *Alderman v. United States* [61] has added tremendous importance to the ultimate disposition of the exclusionary rule issue. *Alderman* held, in a case with national security overtones,[62] that where the Government had *illegally* tapped a defendant's conversation, it was required to turn records of the tap over to the defendant to assure full and fair development of the question whether the tap's fruits were the basis for evidence to be used at trial. *Alderman* rejected the Government's suggestion that a judge should first screen the

---

to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial, hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

18 U.S.C. § 2511(3) (1970).

[58] *See* S. DASH, R. SCHWARTZ, & R. KNOWLTON, THE EAVESDROPPERS 346–62 (1971).

[59] *See* note 27 *supra*.

[60] In the summer of 1969, Attorney General Mitchell indicated that he felt no need to obtain a wiretapping warrant to use wiretapping against, radical, domestic dissident groups. N.Y. Times, July 22, 1969, at 12, col. 1. Revelations of the use of the national security "exception" in taps against the Black Panther Party were made in late 1969. N.Y. Times, Dec. 14, 1969, at 1, col. 1.

[61] 394 U.S. 165 (1969).

[62] Two of the defendants in the cases decided in *Alderman* were accused of espionage. *Id.* at 169.

ults of illegal surveillance *in camera*, and then turn them over to the defense only if they seem "arguably relevant" to the evidence sought to be introduced by the prosecution at trial.[63] If warrantless national security taps or bugs were to be held to violate the fourth amendment, they would be subject to the *Alderman* requirement. In turning the records of such eavesdropping over to defendants, as required by *Alderman*, the Government would be forced to expose to unfriendly parties details of its intelligence operations. The only alternative to such disclosure would be abandonment of the particular prosecution — even if altogether unrelated to the illegal surveillance. Indeed, one in danger of prosecution could put the Government to that choice completely on his own initiative by telephoning or visiting premises believed to be illegally tapped or bugged.[64] For example, if tapping a foreign embassy were illegal, a defendant, about whom the Government had built a case relying on legally obtained evidence, might avoid prosecution by merely placing a call to a foreign official and inquiring into a matter as trivial as the procedure for obtaining a visa.

The *Alderman* Court said these dangers were outweighed by the need for strict enforcement of the exclusionary rule, believing the relevance of a tap or bug to the prosecution's evidence could be determined correctly only in an adversary context with the defendant fully aware of the information revealed by the illegal electronic surveillance.[65] The task of determining arguable relevance to the actual evidence of the often voluminous records of taps was, in the Court's view, too complicated and time consuming for a judge sitting *in camera* to insure that no tainted evidence would be introduced.[66] Thus, unless *Alderman* is overruled at least with regard to national security cases, the Government can avoid the Hobson's choice of disclosure or nonprosecution in cases where the defendant has been subjected to an unlawful[67] national security tap or bug only if it wins its case that warrantless national security electronic surveillance is con-

---

[63] *Id.* at 181.

[64] Government Brief 40.

[65] 394 U.S. at 182–85.

[66] *Id.* at 182.

[67] *Alderman* apparently does not require disclosure of such surveillance to the defendant for the purpose of answering the threshold question of *legality* of the tap or bug. Pursuant to hints contained in two cases decided soon after *Alderman*, Giordano v. United States, 394 U.S. 310, 314 (1969) (Stewart, J., concurring); Taglianetti v. United States, 394 U.S. 316, 317–18 (1969) (per curiam), and pursuant to a statutory grant of discretion, 18 U.S.C. §§ 2518(10)(a), 3504(a)(2) (1970), lower federal courts have sometimes opted to consider the legality question *in camera*. *See, e.g.*, United States v. Butenko, 318 F. Supp. 66, 70 (D.N.J. 1970).

stitutionally permissible — and so not covered by *Alderman* at all.[68]

The essence of the Nixon Administration's claim with regard to national security surveillance is that the practice should be exempted from the customary requirements of the fourth amendment.[69] The executive asserts it can dispense with (1) the requirement that, where practicable, a warrant be obtained from an independent judicial officer;[70] and (2) the demand that a search occur only upon the existence of facts that would lead a reasonable man to believe that evidence of crime is likely to be found at the premises of seizure — probable cause.[71] The argument for departing from the warrant and probable cause requirements rests on two grounds. One involves a claim of inherent unreviewable powers of the President. The other involves interpretation of the fourth amendment.

First, the exercise of presidential power and responsibility as Commander in Chief of the Armed Forces,[72] and as Chief Executive,[73] in maintaining the rule of law domestically [74] and in conducting foreign affairs,[75] is argued to be immune from traditional fourth amendment standards.[76] The foreign affairs power, and even the commander-in-chief power, arguably could justify intelligence gathering against foreign threats by electronic surveillance of foreign government personnel even while they are

---

[68] These alternative positions — overrule *Alderman* in national security cases, or declare national security electronic surveillance constitutional — are advanced by the Government in the domestic security wiretapping case now before the Supreme Court. Government Brief *passim*.

[69] *Id.* at 9–35.

[70] *Id.*

[71] "The traditional standard of probable cause would be wholly inappropriate for testing the reasonableness under the Fourth Amendment of this category of search and seizure." *Id.* at 23. It should be noted that the use of bugged informers, whether or not in a national security context, has been held not to constitute a search and hence not to be subject to any fourth amendment requirements. United States v. White, 401 U.S. 745 (1971); *see* pp. 1273–74 *infra*.

[72] U.S. CONST. art. II, § 2.

[73] U.S. CONST. art. II, § 1.

[74]

> "The President, in his dual role as Commander-in-Chief of the armed forces and Chief Executive, possesses another serious power and responsibility — that of safeguarding the security of the nation against those who would subvert the Government by unlawful means."

Government Memorandum of Law, quoted in United States v. United States Dist. Court, 444 F.2d 651, 658 (6th Cir.), *cert. granted*, 403 U.S. 930 (1971) (No. 1687). This power and responsibility gains additional constitutional support in the mandate that federal authorities guarantee a republican form of government to the states. U.S. CONST. art. IV, § 4.

[75] United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319–22 (1936).

[76] *See* United States v. United States Dist. Court, 444 F.2d 651, 657–58 (6th Cir.), *cert. granted*, 403 U.S. 930 (1971) (No. 1687).

in the United States.[77] Similarly, the need of the Commander in Chief to obtain preventive intelligence on domestic threats to the continued functioning of the Government,[78] as well as the need of a Chief Executive charged with maintaining the rule of law to have such data, might justify electronic surveillance of domestic political dissidents reasonably believed to be a threat to the national security.[79]

The second ground is that the fourth amendment itself does not explicitly require that all searches be conducted upon the issuance of a warrant based on probable cause. Rather, it is argued, only "unreasonable" searches are prohibited,[80] and the clause of the amendment concerning warrants is to be read independently.[81] Where the Government's need to intrude on individual privacy is based on policies other than criminal investigation and prosecution, courts have occasionally read out the probable cause and warrant standards as irrelevant.[82] National security surveillance arguably comes within this class of searches since the need to obtain intelligence to protect the national security from all threats is said to represent a predominantly noncriminal investigatory goal.[83]

It is the purpose of this subsection to evaluate these two grounds. The analysis will proceed in three stages. Each ground will be examined separately; then special considerations that attend relaxation of the judicial warrant requirement, whatever the decision on probable cause, will be considered.

---

[77] *See* United States v. Clay, 430 F.2d 165, 171 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971); United States v. Butenko, 318 F. Supp. 66, 70–73 (D.N.J. 1970).

[78] Reply Brief for Petitioner at 5–7, United States v. United States Dist. Court, 444 F.2d 651 (6th Cir.), *cert. granted*, 403 U.S. 930 (1971) (No. 1687) [hereinafter cited as Government's Reply Brief]. Implementation of the statutory provisions for the use of federal troops in times of extreme domestic unrest, 10 U.S.C. §§ 331–33 (1970), is facilitated by the comprehensive gathering of domestic intelligence. Government's Reply Brief 7.

[79] *See* Government's Reply Brief 5–8.

[80] Government Brief 11; *see* Wyman v. James, 400 U.S. 309 (1971) (warrantless home visit by welfare worker held not violative of fourth amendment on alternative grounds of not being a search and of being a search that was reasonable); Camara v. Municipal Court, 387 U.S. 523, 536–37 (1967) (administrative searches for housing violations must be pursuant to warrant but standard of probable cause does not require probability of violation in any given dwelling).

[81] *See* T. TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 23–24 (1969). The text of the amendment reads as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[82] *E.g.*, Wyman v. James, 400 U.S. 309 (1971).

[83] Government Brief 19.

2. The Extent of Inherent Presidential Authority. — The inherent power argument asserts that, regardless of what the fourth amendment may require, the Executive must be permitted the use of warrantless national security electronic eavesdropping if he is to fulfill his responsibilities as Commander in Chief, in maintaining the rule of law domestically, and in conducting foreign affairs. Each of these three types of responsibility shall be considered in turn, and it shall be shown that none justifies circumvention of the fourth amendment in national security cases in general. But one special type of case — surveillance of foreign government personnel while they are in the United States — may nevertheless be immune to fourth amendment scrutiny.

(a) The Duty as Commander in Chief. — *(i) In the Absence of Hostilities at the Place of Surveillance.* — Little dispute exists over the President's duty as Commander in Chief to operate even in peacetime a wide-ranging intelligence network abroad to protect the nation from foreign attack, from sabotage against military installations, and from espionage which would weaken the nation's defense position. In the exercise of the commander-in-chief power abroad, operations involving the destruction of property and life, which, if carried out at home, would raise the gravest questions of legality, are routinely executed. But this broad executive power stems in part from the Supreme Court's view that aliens outside the territorial jurisdiction of the United States are not entitled to constitutional guarantees.[84]

When the President, even as Commander in Chief, pursues his military policies at home, he customarily does so under far stricter legal constraints.[85] This much was made clear by the Supreme Court's invalidation of President Truman's seizure of the domestic steel mills during the Korean War in *Youngstown Sheet & Tube Co. v. Sawyer*.[86] Although the power exerted by the President over the nation's economy would probably have been constitutionally justifiable had Congress given prior approval,[87] the Court, in the absence of legislative sanction, held that the President's commander-in-chief authority alone did not extend to taking control of material resources at home, even though their disposition had a clear effect on the management of a full-scale war abroad.[88] Had the Court ruled otherwise, all aspects of domestic life arguably affecting the conduct of the

[84] Johnson v. Eisentrager, 339 U.S. 763, 771 (1950) (dictum). Although the case concerned enemy aliens in wartime, the dictum seems to carry the logic of the case far beyond its narrow facts.

[85] *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 642 (1952) (Jackson, J., concurring).

[86] 343 U.S. 579 (1952).

[87] *Id.* at 631 (Douglas, J., concurring).

[88] *Id.* at 587.

rean War abroad would have been susceptible to regulation at the Executive's discretion.[89]

It could of course be argued that *Youngstown* cannot control the question of the power of the Commander in Chief in the national security surveillance area, since the electronic surveillance provisions of the 1968 Crime Control Act colorably provide the President with the congressional authorization he lacked in seizing the steel mills. One answer to that argument, considered more fully below, is that the Act may well not have been intended as affirmative authorization for warrantless eavesdropping.[90] But more to the point, as soon as the President relies on congressional authorization, he is outside his inherent powers, and the constitutionality of the legislation is put in issue. Absent an emergency,[91] the legislation will be judged under traditional constitutional criteria.

(*ii*) *With Hostilities Proximate to the Place of Surveillance.* — Even in wartime and in proximity to hostilities, where fundamental individual rights of a citizen guaranteed by the Constitution have been threatened by the exercise of the Executive's military power, the Court, both before and since *Youngstown*, has been consistently wary of claims of exigency to justify deviations from normal procedure. In the nineteenth century, the Court staunchly upheld the right to a civilian jury trial despite claims that any alternative to a military tribunal would seriously undercut the Government's ability to deal with threats to the Union during the Civil War.[92] Similarly, military seizures of civilian property in wartime have been declared unlawful.[93] In both cases, the Court stressed that only actual emergency — either the actual inability of civil courts to function[94] or the necessity of seizing property lest it fall into enemy hands and assist anti-Government forces[95] — justified bypassing traditional safeguards. Since *Youngstown*, the Court has reiterated this rule that only abnormal circumstances — most typically, the need for quick decisionmaking in a battle zone — justify modifications of such requirements as citizens' rights to a civilian trial.[96] A

---

[89] *Id.* at 642 (Jackson, J., concurring).

[90] *See* p. 1260 *infra*.

[91] *See* pp. 1310–11 *infra*.

[92] *Ex parte* Milligan, 71 U.S. (4 Wall.) 2 (1866); *cf.* Duncan v. Kahanamoku, 327 U.S. 304 (1946).

[93] Mitchell v. Harmony, 54 U.S. (13 How.) 115 (1852). *But see* United States v. Russell, 80 U.S. (13 Wall.) 623 (1872).

[94] *Ex parte* Milligan, 81 U.S. (4 Wall.) 2, 121 (1866); *see* pp. 1322–24 *infra*.

[95] Mitchell v. Harmony, 54 U.S. (13 How.) 115, 134 (1852).

[96] *See* Reid v. Covert, 354 U.S. 1, 19 (1957). *See also* Johnson v. Eisentrager, 339 U.S. 763, 781–85 (1950).

79-064 O - 76 - 42

narrow exception has been made for citizens, not to speak of aliens, who violated the law of war by entering the United States in wartime as combatants — passing surreptitiously from enemy territory into our own as enemy agents and discarding enemy uniforms upon arrival to facilitate the commission of hostile acts.[97] But that narrow exception would seem to have little relevance to the dispute on warrantless national security electronic surveillance, particularly in peacetime.

(*iii*) *Conclusion.* — Thus, while the Court has indicated that constitutional safeguards do not apply with full force to foreigners, at least while abroad,[98] and ordinarily has constricted the rights of American troops [99] or even civilians in the exigencies of wartime decisionmaking,[100] authorization of peacetime, domestic, warrantless eavesdropping would represent a serious new step. For neither Congress nor the executive has presented any indication of actual exigency to justify such a major modification of the fourth amendment.

The insurrection suppression power is operative only when normal law enforcement resources are inadequate.[101] Deferring to the need to plan for that eventuality, while customary investigatory activities continue operating under traditional restraints, underwrites a dual standard for police, leaves citizens uncertain of their liberties, and might well create an excuse to ignore normal procedures altogether. A standard permitting warrantless eavesdropping only where likely to produce information that will shed light on future civil disorder seems too vague to serve as any serious limitation. The duty to command troops against domestic insurrection is only rarely invoked,[102] and seems an attenuated rationale for a continuous and sweeping expansion of executive power.

(*b*) *The Duty to Maintain the Rule of Law at Home.* — Short of actual insurrection, the power and duty of the President to safeguard the domestic security is identical to his ordinary power and duty to enforce the laws.[103] Being defined by the very range of statutes Congress has passed to control private and official conduct,[104] the President's role as a law enforcement officer would not appear to warrant special "inherent power" treatment

---

[97] *Ex Parte* Quirin, 317 U.S. 1 (1942).

[98] *See* Johnson v. Eisentrager, 339 U.S. 763, 771 (1950).

[99] *See id.* at 783.

[100] *See* Hirabayashi v. United States, 320 U.S. 81, 99 (1943).

[101] *See* Government's Reply Brief 23–27.

[102] In this century, state and local officials have requested and received federal military assistance to suppress disorder only eight times. Government's Reply Brief 25–27.

[103] U.S. CONST. art. II, § 3.

[104] *See* Myers v. United States, 272 U.S. 52, 177 (1926) (Holmes, J., dissenting).

by the courts in the particular case of very serious national security crime.[105] Even if some categories of crime (as distinguished from some categories of presidential duty) were such as to warrant extraordinary treatment, one would think that Congress, which has the sole power in the federal government to denominate activity as criminal,[106] would be the branch to make such a decision.

Of course it might be argued that the wiretapping provisions of the 1968 Crime Control Act represent such a specification, but the argument has three serious difficulties. First, the authority granted the executive is sufficiently vague as to serve as no limit whatever.[107] Second, it is possible that the 1968 legislation is not a positive authorization of extraordinary executive power with respect to certain crimes, but rather a mere recognition of illimitable executive power in what amount to emergency circumstances. Finally, even if the legislation did represent a congressional attempt to single out certain crimes for differentiated treatment, the Constitution may not permit any crimes to receive such unique fourth amendment treatment.[108]

In short, the necessity of enforcing the rule of law at home cannot justify circumvention of the fourth amendment for certain classes of crimes.

(*c*) *The Duty to Conduct Foreign Affairs.* — Like the duties of Commander in Chief, the President's treatymaking power and more general authority to conduct the nation's diplomacy have always been viewed as subject to traditional constitutional safeguards for citizens, even when exercised with congressional approval.[109] Although it has been held that states' rights may be infringed by the treatymaking power,[110] the same has never been decided with regard to citizens' rights. Thus, it seems clear that no agreement could be signed with a foreign nation that had the effect of bargaining away the constitutional rights of citizens. And it would seem to follow a fortiori that intelligence gathering in pursuit of effective diplomacy, as merely ancillary to the actual process of negotiation, would be subject to similar restraints.[111]

---

[105] *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Douglas, J., concurring). *But see* Brinegar v. United States, 338 U.S. 160, 183 (1949) (Jackson, J., dissenting).

[106] United States v. Hudson, 11 U.S. (7 Cranch) 32 (1812).

[107] *See* Schwartz, *The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order,"* 67 MICH. L. REV. 455, 491 (1969).

[108] Katz v. United States, 389 U.S. 347, 360 (1967) (Douglas, J., concurring).

[109] *See* Reid v. Covert, 354 U.S. 1, 17–19 (1957).

[110] Missouri v. Holland, 252 U.S. 416 (1920).

[111] *Cf.* New York Times Co. v. United States, 403 U.S. 713 (1971); *The Supreme Court — 1970 Term*, 85 HARV. L. REV. 3, 101 (1971).

(d) *The Inherent Power to Conduct Electronic Surveillance of Foreign Government Officials in the United States.* — It follows from the analysis just conducted that warrantless national security electronic surveillance is in general subject to fourth amendment scrutiny. It might be argued, however, that at the very least, the executive may ignore the fourth amendment to spy on foreign government officials while they are in the United States. Intelligence thus accumulated could facilitate exercise of the foreign affairs powers, and could serve a preparatory and preventive function within the commander-in-chief power.

There is some support for this form of the "inherent power" argument in analogous cases. For example, the courts have granted the executive and Congress unusual discretion in dealing with aliens within American borders: [112] in reviewing standards for immigration and expulsion of aliens, the Court has usually deferred to the other branches, in part on the ground that treatment of foreigners, who for the most part retain foreign citizenship, inevitably involves delicate matters of international relations and is best left beyond careful judicial scrutiny.[113] Similarly, as noted earlier, aliens abroad have been believed beyond constitutional protection of individual liberties.[114] Since the Constitution does not operate extraterritorially to protect foreigners from American intelligence gathering techniques, it might be argued that entry by a foreigner (for example, an embassy or consular official) into the United States should not immunize him against the clandestine intelligence gathering techniques he encounters abroad.[115] Certainly he is likely to be as valuable a source of information; in fact, while working in the United States he may be of special value, since he may be presumed to concentrate his efforts on problems concerning relations between the United States and his nation. Lower courts implicitly have recognized this logic, indicating that foreign intelligence taps were appropriate exercises of the President's power, despite the peacetime, domestic context in which they were conducted.[116]

We shall learn below, however, that the same result might be reached through the fourth amendment itself rather than by circumvention of that provision. And if so reached, the result carries

---

[112] *See* Galvan v. Press, 347 U.S. 522 (1954); Harisiades v. Shaughnessy, 342 U.S. 580 (1952).

[113] Harisiades v. Shaughnessy, 342 U.S. 580, 591 (1952).

[114] *See* Johnson v. Eisentrager, 339 U.S. 763, 771 (1950) (dictum).

[115] Even though an alien gains some rights by crossing the border into the United States, those rights are limited so long as his allegiance to the United States is limited. Johnson v. Eisentrager, 339 U.S. 763, 770 (1950).

[116] *See, e.g.*, United States v. Butenko, 318 F. Supp. 66 (D.N.J. 1970). *See also* Comment, *supra* note 43, at 1248–50.

with it certain limits of "reasonableness" highly protective of individual rights which are absent from any "inherent power" argument. Thus, while perhaps taps of foreign officials in general and certainly eavesdropping on embassies in particular may be deserving of exemption from fourth amendment scrutiny, the better course is probably to subject all executive surveillance by electronic means at home in peacetime to the requirements of that charter.

3. The Reasonableness of Warrantless National Security Electronic Surveillance Under the Fourth Amendment. — The second argument for waiving the normal requirements of a warrant and probable cause is that national security searches, because of the gravity of the threat to which they are addressed, are "reasonable" within the meaning of the fourth amendment's first clause. If so, the second clause's specification of warrants based on a finding of probable cause might not apply with full force, if at all. The thrust of recent years' fourth amendment adjudication, at least where criminal investigations are involved, has been in the opposite direction. The general rule has been that absent "exigent circumstances," revolving around a lack of time to seek a warrant without seriously risking loss of evidence or physical danger,[117] a warrant based on a judicial officer's finding of probable cause is required for the search of a person's premises or person.[118] In most wiretapping and bugging cases, investigators have sufficient time to obtain judicial approval.[119]

The Supreme Court has recognized two classes of exceptions to this refusal to split the two clauses of the fourth amendment. The remainder of this subsection is directed to the inquiry whether either of those exceptions covers domestic national security elec-

[117] In the criminal area the Supreme Court has dispensed with the warrant requirement in cases presenting situations where there is no time to obtain a warrant and still be relatively certain that the items sought will not have been moved or destroyed in the interim. Schmerber v. California, 384 U.S. 757, 770–71 (1966) (lack of warrant to take defendant's blood sample to determine whether he was intoxicated was excused because delay would have entailed destruction of the evidence); Carroll v. United States, 267 U.S. 132 (1925) (warrantless search of vehicle upheld because of danger that vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought); Warden v. Hayden, 387 U.S. 294 (1967) (warrantless search held valid when conducted in hot pursuit of armed felon). Another exception, in permitting a limited search incident to arrest, reflects a concern for the safety of arresting officers. Chimel v. California, 395 U.S. 752 (1969).

[118] "[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment." Katz v. United States, 389 U.S. 347, 357 (1967).

[119] Where there is not sufficient time, even the statutory standards, strict with regard to exhaustion of nonelectronic methods, make provision for warrantless electronic surveillance. 18 U.S.C. § 2518(7) (1970).

tronic surveillance. The analysis will be in four steps. First, each of the two exceptions will be separately treated and will be found inapplicable to national security electronic surveillance in general. In a third stage, the possibility that first amendment considerations reinforce the inapplicability of the two exceptions will be considered. Finally the subsection shall inquire, again, whether and to what degree the case of foreign government officials in the United States may be different — whether it may warrant splitting the two clauses of the fourth amendment even if other cases of national security electronic surveillance do not.

(*a*) *The First Exception*: Camara *and* James. — In several situations involving implementation of government policies other than criminal investigation, the Court has rejected the warrant requirement [120] and relaxed the probable cause standard [121] on the ground that even without them, the search at issue was reasonable. The Court in these cases reasoned that the intrusion at issue was less severe than the typical criminal search which involves an unexpected, deliberate rummaging through a given premises for specific items of property followed by at least temporary confiscation.[122] In *Wyman v. James*, for example, the Court not only stressed that the primary purpose of the mandatory welfare case worker's home visit was "rehabilitative" and noncriminal, but also pointed out in rejecting the warrant requirement and the probable cause standard that the visits were announced beforehand and did not entail any rummaging about the recipient's premises.[123] *Camara v. Municipal Court* required prior judicial approval for housing code inspections, but did not insist on probable cause to believe a violation or crime existed. Instead, the Court was satisfied with a showing by government officials that "reasonable legislative or administrative standards for conducting an area inspection [were] satisfied with respect to a particular dwelling." [124] In each case, the Court purported to weigh the purpose and the need to maintain the program of official intrusions against the degree of infringement of citizen privacy in deciding whether probable cause or the prior approval requirements should be maintained.

Many of the cases which seem to fall within the Government's national security claim, however, do not seem suited to the kind of allowance the Court granted in either *Camara* or *James*. National security taps of domestic-based threats to the structure of

[120] *See* Wyman v. James, 400 U.S. 309 (1971).

[121] *See* Camara v. Municipal Court, 387 U.S. 523 (1967).

[122] *See* Wyman v. James, 400 U.S. 309, 317–18 (1971); Camara v. Municipal Court, 387 U.S. 523, 530 (1967).

[123] 400 U.S. at 317–18.

[124] 387 U.S. at 538.

government would seem to involve inextricably and inevitably a policy of criminal law enforcement; those who pose serious threats will doubtless be tried when they are discovered. It would seem impossible to conceive of any serious threat to the nation's security from within that did not involve a criminal violation. While national security surveillance might conceivably focus on law-abiding dissident leaders on the grounds that they can provide information useful in heading off major disorder,[125] the ultimate purpose of such intrusions remains crime-oriented, even if in a preventive rather than prosecutorial sense.

(*b*) *The Second Exception*: Terry v. Ohio. — In a narrow class of cases, the Court has authorized limited warrantless police searches of citizens for purposes of crime prevention where probable cause was absent. *Terry v. Ohio*[126] upheld a limited pat-down frisk for dangerous weapons in a street situation where a police officer, though lacking probable cause, suspected impending criminal activity. The search upheld was viewed as "reasonable" because it did not involve delving into a suspect's pockets for evidence, but rather was commensurate with its purpose of preventing harm to a police officer.[127] But no considerations such as those which justified the limited search without probable cause or warrant in *Terry* seem applicable where electronic surveillance is at issue. A national security tap or bug is no less intrusive than a tap or bug authorized under the ordinary warrant procedure. At best it might be argued that, by analogy to the situation where a policeman feels threatened in the street, certain activities by, say, political dissidents pose such inordinate dangers to the community that customary restraints exerted on police investigatory techniques by the probable cause requirement should be relaxed. The Government, however, has made no attempt statutorily or in litigation to specify such activities. Rather, it has argued for a virtually undefined class of national security threats, the limits of which can be determined only by almost unreviewable executive discretion.[128] Indeed, even if specification of particularly dangerous activities were attempted, it is again arguable that the Constitution forbids singling out any crime for special treatment.[129]

(*c*) *The Inapplicability of the Two Exceptions: First Amendment Considerations.* — There is an additional reason that the intrusion represented by electronic surveillance aimed at domestic

---

[125] *See* p. 1278 *infra*.

[126] 392 U.S. 1 (1968).

[127] *Cf.* Chimel v. California, 395 U.S. 752 (1969).

[128] Government Brief 22–23.

[129] *See* pp. 1259–60 & note 108 *supra*.

threats to the national security is too serious to be covered by either the *Camara-James* or the *Terry* exception to the warrant and probable cause requirements. That is, that such surveillance could threaten first amendment rights by deterring citizens from engaging in private associational activities which the Government is likely to tap or bug.[130] The historical background of the fourth amendment,[131] as well as a set of recent decisions,[132] demonstrates that maintenance of traditional search and seizure safeguards has been motivated partly by fears that political activity might easily be suppressed in their absence.[133]

Any surveillance of associational activities can "chill" their vigor.[134] Electronic eavesdropping is especially dangerous in this regard, because of its capacity to "chill" the activities of politically respectable leaders — say, of a minority group — who make no practice of operating clandestinely (*i.e.*, away from the telephone) or transiently. Such leaders have little to fear from other forms of surveillance, *e.g.*, informers, since their associational activities are conducted in the open. The Government might, however, attempt electronic surveillance of such leaders with a national security justification: it might be asserted, for example, that data gleaned from taps and bugs on such citizens could improve police preparation for pending disorder. Any such arguable advantage would need to be balanced against the chilling effects imparted by the surveillance and against the danger that collected data could be misused; [135] for example, the eavesdrop-

[130] *See generally* Note, *Eavesdropping at the Government's Discretion — First Amendment Implications of the National Security Eavesdropping Power*, 56 CORNELL L.Q. 161 (1970).

[131] *See, e.g.*, Entick v. Carrington, 19 How. St. Tr. 1029 (1765) (general warrant for seizure of political papers held contrary to common law).

[132] *See* Stanford v. Texas, 379 U.S. 476, 485 (1965) (search warrant for the books and records of the Communist Party held insufficiently specific in describing objects to be seized; suggests that "the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas they contain"); Marcus v. Search Warrant, 367 U.S. 717, 729 (1961) (declaring warrant for search for obscene literature insufficiently specific and noting that "unrestricted power to search and seizure could also be an instrument for stifling liberty of expression").

[133] Although these cases dealt with the dangers of wholesale suppression of publications that were seditious, Stanford v. Texas, 379 U.S. 476 (1965), and obscene, Marcus v. Search Warrant, 367 U.S. 717 (1961), and with the need for warrants to describe with particularity the items to be seized, the cases' underlying concern with political suppression seems equally applicable in the context of wiretapping, at least so far as to maintain the traditional probable cause standard for intrusion.

[134] *Cf.* pp. 1274–77 *infra*.

[135] *See* Comment, *Preventive Intelligence Systems and the Courts*, 58 CALIF. L. REV. 914, 925 (1970); pp.1275–76 *infra*.

ing might uncover information useful in attacking dissidents politically, as in the case of the FBI taps on Martin Luther King, Jr.[136] On balance, first amendment considerations at least reinforce the case against applying the *Camara-James* or *Terry* exceptions to electronic eavesdropping for national security.

(*d*) *The Reasonableness of Electronic Eavesdropping on Foreign Government Officials in the United States.* — The fourth amendment analysis thus far has been confined to domestic threats to the national security, cases inevitably linked with criminal activity. It remains to be asked whether an exception analogous to that in *Camara* and *James* might be carved out for national security eavesdropping unconnected with crime — for instance, bugs or taps on foreign officials while they are in the United States, whether on the embassy or on nonembassy residences and telephones. Where electronic surveillance is utilized for predominantly noncriminal purposes — in this instance, to gather intelligence useful in diplomatic and military planning — it does not necessarily follow that the probable cause standards should be dispensed with. To be sure, if surveillance in such cases were permitted only where there was probable cause that a search would turn up criminal evidence, the Government would lose access to a valuable source of foreign intelligence. But it is difficult to argue for an exception analogous to that in *Camara* and *James* when the intrusion may be considered as great as in a criminal search.

Two other considerations, however, suggest that the courts might well be willing to legitimate some warrantless electronic surveillance for foreign and military intelligence purposes in much the same way housing inspections were aproved in *Camara*. First, electronic eavesdropping is probably an indispensable way to understand the evolution of a foreign nation's posture toward the United States. Especially where matters regarding military preparedness are concerned, the technique is of doubtless utility in discovering information that is unlikely to be openly discussed or publicized: the foreign nation's own intelligence activities aimed at uncovering American policy shifts and secrets and upcoming or possible changes in position by the foreign state on a broad range of international issues. Second, because of the practice's utility, the Government is likely to maintain a program of electronic surveillance, whatever the Supreme Court rules.

Presumably out of deference to these two considerations, lower courts have indicated that warrantless taps of aliens for foreign intelligence purposes are legal and thus their records need

---

[136] *See* V. NAVASKY, KENNEDY JUSTICE 137–38 (1971).

not be disclosed in *Alderman* hearings.[137] Legalization of foreign *embassy* taps exclusively might be justified on the ground that their impact on privacy will be concentrated in large part on aliens, to whom in certain circumstances the Supreme Court has refused the protection given citizens of a judicially authorized warrant based on probable cause.[138] Indeed, not only would the impact of embassy taps be confined to aliens, but it would be minimal even on their senses of privacy. For embassy personnel probably anticipate, far more than American citizens, that they will be placed under sharp, even uncomfortable scrutiny for hints as to their governments' policies. In fact, they probably assume that American officials abroad suffer the same risk and are likely to regard reciprocal use of the technique as among the "rules of the game" of international politics.

Still, to legalize bugs or taps of foreign embassies or foreign officials' homes on the likelihood that intelligence information will be captured authorizes intrusions into a large number of conversations to which citizens will be parties.[139] While some of these conversations, as where American consultants to foreign governments are concerned, will doubtless yield information useful in diplomatic or military planning, others will involve purely private matters. In either event, the Government will amass information about citizens without being constrained by ordinary constitutional safeguards. This problem will be especially acute in taps or bugs of nonembassy residences or phones of foreign officials, which are particularly likely to uncover private matters concerning citizens.

Thus, approving foreign intelligence taps and bugs according to any standard less stringent than that required for criminal searches will inescapably multiply government intrusions on citizen privacy. Moreover, since many citizens who talk to foreign officials are likely to discuss political issues, a liberalized tapping and bugging policy would pose the danger of government misuse of such potentially charged information, since it may be recorded and stored in permanent investigatory files.[140]

---

[137] *See* United States v. Clay, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971); United States v. Butenko, 318 F. Supp. 66 (D.N.J. 1970).

[138] Abel v. United States, 362 U.S. 217, 232–33 (1961) (court upholds arrest of alien pursuant to administrative warrant of Immigration Service).

[139] At least one case has authorized citizens to assert rights incidentally infringed by government treatment of an alien. Mandel v. Mitchell, 325 F. Supp. 620 (E.D.N.Y. 1971), *prob. juris. noted*, 92 S. Ct. 670 (1972) (No. 71–16) (invitors and expectant audience of Belgian Marxist scholar-lecturer successfully challenge constitutionality of his exclusion from United States by Attorney General); *see* pp. 1154–1159 *infra*.

[140] *Cf.* pp. 1274–77 *infra*.

Accommodating the need to protect citizen privacy and the Government's practice of obtaining foreign intelligence through bugs and taps is hardly easy. Openly legitimating embassy taps and bugs as inherently "reasonable" would force citizens (and foreign officials) to avoid those settings when they wanted to discuss serious matters. However, the costs thus imposed on citizens' freedom to discuss their affairs at their own convenience do not seem especially high. As for eavesdropping on foreign officials at settings outside the embassies, where citizen-foreigner contact, especially of a private nature, is more likely to occur, a system of prior approval might be designed to minimize intrusions on citizen privacy. For example, taps and bugs could be authorized only where, on the basis of embassy taps, bugs, or other sources of information, it seemed probable that the conversation at issue would not include citizens and would yield information pertaining to the foreign nation's diplomatic or military policy. The possibility of such circumscription is indeed an arguable advantage of authorizing eavesdropping on foreign officials in the United States through fourth amendment "reasonableness" rather than through an "inherent power" argument.

4. Some Special Considerations Attending Authorization of Electronic Surveillance by the Attorney General. — Relaxation or elimination of the requirement that a neutral judicial official approve any electronic surveillance in advance, whether founded on fourth amendment "reasonableness" or on an "inherent power" argument, imports some different considerations than does relaxation of the probable cause standard, and therefore merits separate treatment. The government argument on prior judicial approval is that, whatever the standard adopted by the courts for national security electronic surveillance, it should be applied by the Attorney General.[141] The judiciary is said to lack competence in judging when such surveillance is justified under fourth amendment standards, or is "reasonable" under the statutes.[142] Furthermore, the Government's interest in secrecy might be threatened if judges were permitted to screen taps and bugs beforehand.[143] Finally, allowing the Attorney General, rather than a variety of federal judges, to authorize national security taps is said to be likely to lead to more uniform application of the criterion.[144]

As a general matter, requiring prior judicial approval, whatever standard exists to regulate national security surveillance, seems likely to provide greater protection for individuals' privacy

[141] Government Brief 19.

[142] *Id.* at 25.

[143] *Id. See also* Brownell, *supra* note 37, at 210.

[144] Government Brief 26–27.

than does requiring administrative approval.[145] As recently as last Term, the Supreme Court held that approval by an executive official with a stake in the surveillance or intrusion at issue is an inadequate substitute for the scrutiny of a judicial officer, who is presumed to view the necessity for the requested search more disinterestedly and thus is likely to make a fairer judgment of its utility.[146] The existence of post hoc judicial review has long been believed an inadequate constraint on police illegality; the fruits of many taps, when exposed, place serious pressure on judges to admit them.[147] In the area of national security surveillance, moreover, many taps and bugs, because they will not be used as criminal evidence or capture conversations of criminal defendants, would never be reviewed. In all, enforcement of a strict prior approval requirement is likely to reduce significantly government abuse of the technique — and its availability is one arguable advantage of authorizing some national security electronic surveillance through fourth amendment "reasonableness" rather than through an "inherent power" argument.

As for the need for secrecy, the Government's claim seems overstated. If not magistrates, then certainly presidentially appointed federal judges can be trusted to keep secret the information they are given in what is typically a secret, *ex parte* hearing.[148] Second, even the post-search review the Government contemplates when it is forced to plead the surveillance's legality [149] would necessarily divulge at least some of the circumstances behind the intercept in order for the "clear abuse" standard to be applied.[150]

The additional argument that an Attorney General's approval

---

[145] *See* Johnson v. United States, 333 U.S. 10, 14 (1948); *The Supreme Court — 1970 Term*, 85 HARV. L. REV. 3, 239–41 (1971).

[146] Coolidge v. New Hampshire, 403 U.S. 443 (1971). *But see* Note, *Police Practices and the Threatened Destruction of Tangible Evidence*, 84 HARV. L. REV. 1465, 1471 n.29 (1971). On the general tendency of the executive to overrate threats to national security, see Section II *supra*.

[147] *See* Beck v. Ohio, 379 U.S. 89, 96 (1964). *But see* Note, *supra* note 146, at 1469–70.

[148] *See* p. 1223 *supra*. In United States v. United States Dist. Court, 444 F.2d 651 (6th Cir.), *cert. granted*, 403 U.S. 930 (1971) (No. 1687), the court suggested that if a warrant requirement poses a serious problem of indiscreet judges, a system could be devised whereby the Chief Judge of a Court of Appeals, a high presidential appointee and presumably not a security risk, would alone be authorized to pass on national security wiretap applications. *Id.* at 667. The electronic surveillance legislation enacted in 1968 itself recognizes the possibility of such appellate-level authorization. 18 U.S.C. §§ 2510(9), 2518 (1970).

[149] Government Brief 21.

[150] Nowhere is it argued that in an evidentiary challenge, the court should refrain from at least an *in camera* examination of the basis for the Government's national security claim. *See* Government Brief 23.

is likely to lead to more uniform application of the standard in question also seems exaggerated. The office of Attorney General changes hands every few years; its occupants are likely to have differing perspectives on the need for vigilance against all conceivable national security threats. Even with a single Attorney General, real uniformity may be a chimera: in current wiretap warrant applications, required to be authorized by the Attorney General or designated Assistant Attorneys General,[151] there is evidence that the Attorney General has delegated his responsibility to subordinates.[152] Finally, uniformity, while desirable for the predictability it may lend to the technique, is probably worth sacrificing where, as here, the standard is not clearly communicated to the public and where it poses the threat of more unjustified intrusions on personal security than if a judicial officer screened government applications.

To be sure, it might be contended that courts are ill fitted to determine whether a given intercept is "likely" to yield intelligence information — if such a standard is adopted. What constitutes useful intelligence — as opposed to evidence of crime, where the customary probable cause standard is at issue — is a finding that is beyond usual judicial responsibilities.[153] But the probable result of courts' uncertainty, and of their unfamiliarity with evaluating possible "leads" to intelligence, will merely be reluctance to refuse government applications that seem colorable. Indeed, embassy taps and bugs in particular, because of the frequency of their employment and the likelihood that the Government will be able to argue that any such intercept is as likely as any other to yield useful information, probably should not require prior approval by a court at all. And even on other classes of national security eavesdropping, judicial bias is sure to favor the executive in questionable cases. The Government will thus have lost little through imposition of a warrant requirement. The possibility that courts will occasionally reject government applications and place pressure on officials to justify their activities will provide a modicum of assurance to citizens that national security surveillance is not merely a blank check.

B. Informers

The use of Government-directed informers is believed by government officials to be essential in the investigation of dissident

[151] 18 U.S.C. § 2516(1) (1970).

[152] *See* United States v. Robinson, 10 CRIM. L. REP. 2281 (5th Cir. Jan. 12, 1972) (application for electronic surveillance court order held invalid because authorized by Deputy Assistant Attorney General and not Attorney General or designated Assistant Attorney General). *See also* United States v. Aquino, 10 CRIM. L. REP. 2369 (E.D. Mich. Jan. 17, 1972).

[153] Government Brief 25.

groups they consider a threat to national security.[154] Infiltration of such political groups, however, poses a danger to civil and political rights that is not presented by similar surveillance of nonpolitical, criminal activity.[155] In both contexts the Government is free to intrude as it will, since the use of paid informers is a matter of informal agency determination, not controlled by statute, court decision, or published agency regulation. But experience indicates a special risk in the national security area — a grave potential for agencies exercising unfettered discretion to use the argument of national security in justifying infiltration of dissident political groups from which there is no reasonable expectation of criminal activity.[156] The danger that such political infiltration will interfere with first amendment rights of association[157] demands that it be clearly justified by the governmental purpose that it serves.

---

[154] "[T]he FBI must utilize the services of informers . . . within subversive organizations." Hoover, *The Confidential Nature of FBI Reports*, 8 SYRACUSE L. REV. 2, 6 (1956). "Operating within organizations which seek the destruction of our form of government, these men and women help the FBI to identify internal enemies of our Nation, gather evidence concerning illegal acts by subversives, and obtain intelligence information essential to protecting America's security." *Id.* at 7.

[155] This includes gambling and the sale of narcotics. *See* M. HARNEY & J. CROSS, THE INFORMER IN LAW ENFORCEMENT 17–19 (1960); P. WESTON & K. WELLS, CRIMINAL INVESTIGATION 172–74 (1970). Aside from the FBI, *see* Wall, *Special Agent for the FBI*, N.Y. REV. BOOKS, Jan. 27, 1972, at 14, agencies such as the Food and Drug Administration and the Internal Revenue Service make use of both informers and undercover agents. *See Hearings on Invasions of Privacy (Government Agencies) Pursuant to S. Res. 39 Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 89th Cong., 1st Sess., pt. 2, at 419–23 (1965); *id.* pt. 3, at 1149–50.

In contrast to the use of informers, warrantless electronic surveillance is distinctively a national security technique. Under 18 U.S.C. §§ 2510–20 (1970), the only situations in which warrantless electronic surveillance is not expressly prohibited, other than those in which one of the participants in the conversation has consented to the use of such surveillance, 18 U.S.C. § 2511(2)(c)–(d) (1970), are those involving the national security, 18 U.S.C. § 2511(3) (1970), and those which present problems of temporal exigency. 18 U.S.C. § 2517 (1970).

[156] Testimony at recent hearings conducted by Senator Ervin into Army involvement in domestic surveillance activities indicated that a military intelligence agent's assignment to infiltrate an organization whose purpose it was to coordinate young adult activities in Colorado Springs apparently had been based wholly on the suspicion that members of the group might influence servicemen against the Army in general and the Vietnam war in particular. *Hearings on Data Banks, Computers and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess., pt. 1, at 305–10 (1971) [hereinafter cited as *Constitutional Rights Hearings*]. Indication from the agent's work that even such suspicions were unfounded did not result in the termination of the infiltration. *Id.* at 306.

[157] *See* pp. 1274–77 *infra*.

Informers have been used for national security reasons throughout the twentieth century. They were deployed to combat what was perceived to be an internal threat from radicals during the early 1920's.[158] When fears began to focus on Communism, groups thought to have some connection with the Communist Party were heavily infiltrated. Infiltration of the Party itself was so intense that one former FBI agent estimated a ratio of one informant for every 5.7 members in 1962.[159] More recently, attention has shifted to militant antiwar and civil rights groups. In part because of support for such groups among university students throughout the country, informers seem to have become ubiquitous on campus.[160] Some insight into the scope of the current use of informers was provided by the Media Papers, FBI documents stolen in early 1971 from a Bureau office in Media, Pennsylvania. The papers disclose FBI attempts to infiltrate a conference of war resisters at Haverford College in August 1969, and a convention of the National Association of Black Students in June 1970.[161] They also reveal FBI endeavors "to recruit informers, ranging from bill collectors to apartment janitors, in an effort to develop constant surveillance in black communities and New Left organizations."[162] In Philadelphia's black community, for instance, a whole range of buildings "including offices of the Congress of Racial Equality, the Southern Christian Leadership Conference [and] the Black Coalition"[163] was singled out for

---

[158] In a 1920 report signed by, among others, Roscoe Pound, Zechariah Chafee, and Felix Frankfurter, it was indicated that "[a]gents of the Department of Justice have been introduced into radical organizations for the purpose of informing upon their members or inciting them to activities; these agents have been instructed from Washington to arrange meetings upon certain dates for the express object of facilitating wholesale raids and arrests." NATIONAL POPULAR GOVERNMENT LEAGUE, REPORT UPON THE ILLEGAL PRACTICES OF THE UNITED STATES DEPARTMENT OF JUSTICE 3 (1920).

[159] Levine, *Hoover and the Red Scare*, 195 NATION 232, 233 (1962). For an example of the use of an informer in revealing an individual's affiliation with a Communist-oriented organization, *see* Marzani v. United States, 168 F.2d 133, 140 (D.C. Cir.), *aff'd by an equally divided Court*, 335 U.S. 895 (1948), *aff'd on rehearing by an equally divided Court*, 336 U.S. 922 (1949). According to one commentator, a former FBI agent, the FBI as early as 1940 had decided that "[t]he development of informants within the [Communist P]arty was to be the instrument of its ultimate destruction." Levine, *supra* at 233.

[160] After interviewing campus personnel at several universities, one reporter felt that because of law enforcement officials' dual efforts to enforce drug laws and to keep a watch on radical activities, "undercover activity is now almost a permanent institution on the American college scene." N.Y. Times, March 27, 1971, at 1, col. 5.

[161] N.Y. Times, March 25, 1971, at 1, col. 1.

[162] N.Y. Times, April 8, 1971, at 22, col. 1.

[163] *Id.*

surveillance by building employees and other similar informers working for the FBI.

Although charges of extensive government undercover activity are common, the Media Papers indicated a degree of surveillance greater than had been generally appreciated.[164] Public ignorance of the use of informers underscores the complete absence of visible controls on the practice.

The Supreme Court thus far has rejected claims that fourth amendment restraints on searches and seizures apply to informers.[165] In *Hoffa v. United States* [166] the Court held that an informer's testimony about conversations of the defendant could not be considered the product of a search [167] — and thus was admissible evidence — because the defendant had consented to the informer's presence. In dismissing the argument that the informer's failure to disclose his true purpose vitiated the defendant's consent, Justice Stewart's opinion for the Court held that the fourth amendment does not protect a citizen's belief that "a person to whom he voluntarily confides his wrongdoing will not reveal it." [168] "The risk of being . . . betrayed by an informer . . . is the kind of risk we necessarily assume whenever we speak." [169]

Although *Hoffa* was widely criticized for a failure to give sufficient weight to a person's tendency in certain situations to assume that his words are privately spoken,[170] the current strength of its holding is undiminished. Last term in *United States v.*

---

[164] *See* N.Y. Times, March 25, 1971, at 1, col. 1.

[165] Some protection has been afforded on other grounds. Surreptitious interrogation of a defendant by a wired-for-sound informer after the defendant has been indicted and in the absence of counsel has been held to violate the defendant's sixth amendment right to counsel. Massiah v. United States, 377 U.S. 201 (1964). *Massiah* applies as well to situations not involving the use of electronic equipment. Beatty v. United States, 389 U.S. 45 (1967), *rev'ing per curiam* 377 F.2d 181 (5th Cir. 1967); 41 U. COLO. L. REV. 261, 268 (1969). Furthermore, entrapment by an informer is a defense to a criminal charge. However, entrapment is held to occur only when the informer induces "an *otherwise unwilling* person to commit a criminal act." Sherman v. United States, 356 U.S. 369, 371 (1958) (emphasis added). *See generally* Orfield, *Defense of Entrapment in the Federal Courts*, 1967 DUKE L.J. 39. Finally, dicta in several cases suggest that under some undefined circumstances the use of informers might violate the guarantees of due process by being contrary to the "decencies of civilized conduct." United States v. DeSapio, 435 F.2d 272, 282 (2d Cir. 1970); *see* Hoffa v. United States, 385 U.S. 293, 310–12 (1966). No informer case, however, has actually found such a violation.

[166] 385 U.S. 293 (1966).

[167] *Id.* at 300–03.

[168] *Id.* at 302.

[169] *Id.* at 303.

[170] *See, e.g., The Supreme Court, 1966 Term*, 81 HARV. L. REV. 69, 193–94 (1967). *See also* Note, *Judicial Control of Secret Agents*, 76 YALE L.J. 994 (1967).

White [171] the Supreme Court expressly reaffirmed and expanded *Hoffa*, in holding that the warrant requirement did not apply to evidence obtained from informers carrying transmitters that simultaneously broadcast their conversations with a subject of investigation. In approving bugged informers, the Court rejected claims that the broad rationale of *Hoffa* required modification in light of *Katz v. United States*,[172] which had held that a warrantless bug of a conversation from a phone booth violated a "justifiable" expectation of privacy.[173] *Katz* was deemed inapplicable when the bug or tape recorder was carried by an individual to whose presence the defendant had consented; whether consent was obtained through deception was irrelevant for fourth amendment purposes.

Given the Court's determination that the use of informers does not constitute a search, no need has arisen to draw lines between national security informing and informing not related to the national security in applying fourth amendment law. There remains, however, the possibility, unexplored by the Supreme Court, that infiltration of dissident political groups on grounds that they threaten national security may offend first amendment rights.

1. First Amendment Interests Affected. — When statutes or administrative practices have unnecessarily "chilled" associational activities, the Supreme Court has invalidated them.[174] The cases thus far decided have involved subjection to the risk of governmental sanction [175] or to public obloquy and harrassment [176]

---

[171] 401 U.S. 745 (1971).

[172] 389 U.S. 347 (1967).

[173] Even Justice Harlan, who strongly dissented from the Court's holding in *White*, indicated that it was the electronic equipment rather than the use of the informer that motivated his dissent. 401 U.S. at 784–85.

[174] *See* Dombrowski v. Pfister, 380 U.S. 479, 486–87 (1965). For a general discussion of the freedom of association, see Emerson, *Freedom of Association and Freedom of Expression*, 74 YALE L.J. 1 (1964). The term "chilling effect" was first used in a Supreme Court opinion in Wieman v. Updegraff, 344 U.S. 183, 195 (1952) (Frankfurter, J., concurring). *See generally*, Note, *The Chilling Effect in Constitutional Law*, 69 COLUM. L. REV. 808 (1969).

[175] *See, e.g.*, United States v. Robel, 389 U.S. 258 (1967) (statute imposing criminal penalty on defense facility employee because he was member of a Communist action organization held overbroad); Aptheker v. Secretary of State, 378 U.S. 500 (1964) (statute prohibiting member of Communist organization from using passport held overbroad).

[176] *E.g.*, Shelton v. Tucker, 364 U.S. 479 (1960) (compelling teachers as condition of employment to disclose their membership in organizations held to violate their freedom of association); Bates v. City of Little Rock, 361 U.S. 516 (1960) (compulsory disclosure of NAACP membership lists held unjustified interference with members' freedom of association); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958) (requirement to disclose group membership list held to violate first amendment, in part because of chilling effect on group members).

on account of protected associational activity. To give first amendment protection against informers would be an extension of current law, since the use of informers is not in itself a sanction, nor does it normally pose a serious risk of later government sanctions against protected political activity or of exposure of associational activity to the public at large.

Still, the unrestrained infiltration of dissident political groups may create chills closely analogous to those the Court has already recognized. Information obtained by informers may be used by state and federal agencies, or by private individuals and institutions, to impose sanctions such as denial of employment, credit, or a license on the basis of protected association.[177] State and federal agencies receive information directly from the FBI. Although most of this information consists of criminal records, the description of stolen goods, and the names of fugitives,[178] the federal statute [179] and official regulation [180] which authorize such disclosures speak in very general terms: some information obtained by informers and unrelated to crime may be disseminated.[181] As

[177] *Cf.* pp. 1169–70 *supra*.

[178] For instance, the National Crime Information Center, a computerized index of law enforcement information operated by the FBI, accessible to state, federal and local agencies, and having a capacity of 2.5 million active files, contains "records on wanted persons, stolen vehicles, vehicles wanted in felonies, and other identifiable stolen property, including firearms and stolen securities." *Constitutional Rights Hearings*, pt. 1, at 914. It apparently does not contain surveillance information that is not crime-related.

[179] "The Attorney General shall acquire, collect, classify, and preserve identification, criminal identification, crime, and other records; and exchange these records, with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and other institutions." 28 U.S.C. § 534(a) (1970).

[180] 28 C.F.R. § 0.85 (1971) provides that the Director of the Federal Bureau of Investigation shall undertake the acquisition, collection, and exchange of identification records voluntarily submitted on a mutually beneficial basis by "law enforcement and other governmental agencies, railroad police, national banks, member banks of the Federal Reserve System, FDIC-Reserve-Insured Banks, and banking institutions insured by the Federal Savings and Loan Insurance Corporation."

[181] The degree to which access to surveillance information is given to local agencies appears to be at least in part a function of the warmth of the informal working relationship that exists between the local agency and the Bureau office in that particular locality. Interview with Robert Wall, Former FBI Agent, by telephone from Buffalo, N.Y., January 27, 1972. Dissemination may be restricted to some extent, however, by a recent court decision. Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971), in order to avoid serious constitutional questions, held that 28 U.S.C. § 534 (1970) should be construed to authorize the dissemination of *arrest* records only to federal agencies for the purpose of employment investigations and to law enforcement agencies. 328 F. Supp. at 727–28. The opinion did not treat nonarrest-related surveillance information, but its logic might be thought to demand that the dissemination of such information be at least as restricted.

to private individuals and institutions, the FBI has been scrupulous (with a few notable exceptions [182]) in not providing them with information directly.[183] But they may receive information secondhand from local agencies that deal directly with the FBI,[184] despite the power of the Bureau to revoke an agency's right to receive information on a finding of misuse.[185]

Fears that gathered information may be improperly used are plausibly deepened by an inability to insure or review the accuracy of that information. Although federal legislation has been passed giving an individual some access to credit bureau files kept on him,[186] subjects of government investigatory files based on informer information could not be given such a right of access without compromising the cover of the informers themselves. Thus, individuals interested, for instance, in attending an introductory meeting of a dissident group in order to determine whether they want to join might be deterred by the fear that mere attendance would, however inaccurately, brand them as members in the eyes of an informer. With no opportunity to correct the inaccuracy, or indeed even to know of its existence, an individual's feelings of vulnerability to the improper use or dissemination of "mis"-information are likely to increase.

[182] For instance, an FBI agent without FBI approval supplied confidential information to *Look* magazine in connection with its article on the activities of Mayor Joseph Alioto of San Francisco. *Constitutional Rights Hearings*, pt. 1, at 604. FBI Director Hoover made available to selected newsmen and Congressmen transcripts of the tapped conversations of Martin Luther King, Jr. V. NAVASKY, KENNEDY JUSTICE 153–54 (1971). On another occasion, in reacting to a Trans World Airlines pilot's criticism of the FBI, Hoover explicitly drew on the pilot's FBI files in a caustic letter to the president of TWA. A. Neier, The Dissemination of Derogatory Data by the FBI 29, Oct. 29, 1971 (unpublished paper delivered at conference on the FBI sponsored by the Committee for Public Justice; on file at the *Harvard Law Review*).

[183] *See* Menard v. Mitchell, 328 F. Supp. 718, 722 (D.D.C. 1971). Nevertheless, prior to the Court order in *Menard* to the FBI to limit the dissemination of arrest record information outside the federal government to law enforcement agencies only, such information had been distributed pursuant to 28 CFR § 0.85 (1971) to institutions such as FDIC-insured banks. 328 F. Supp. at 722. *See generally* Hoover, *supra* note 154.

[184] Judge Gesell noted in Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971), that it is "apparent that local agencies may on occasion pass on arrest information to private employers." *Id.* at 722.

[185] According to 28 U.S.C. § 534(b) (1970), "[t]he exchange of records . . is subject to cancellation if dissemination is made outside the receiving departments or related agencies." However, in the pretrial examination in *Menard*, the Chief of the Technical Section of the FBI's Identification Division indicated that there is no procedure by which the FBI inquires into the uses to which arrest information is put by receiving agencies. Neier, *supra* note 182, at 10. The *Menard* proceeding revealed that within the past ten years only six agencies have had their authority to receive arrest information withdrawn. *Id.* at 11–12.

[186] 15 U.S.C. § 1681g (1970).

Even apart from the issues of use and dissemination of information, the use of informers in itself may exercise a chill on protected political activities. In a public political endeavor, where an individual voluntarily exposes his actions to the world, the mere fact of being watched by a government agent probably would not chill his associational activities. However, where individuals attempt to conduct their activities in private, they may understandably be deterred by a fear of informers; a decision to meet in private reflects a desire to restrict the parties with whom one shares information and experiences,[187] to share certain ideas and emotions exclusively with people in whom one feels a sense of trust. Where the atmosphere of trust at a private political meeting is susceptible to erosion by the feared presence of an informer, attendance at the meeting may be deterred, and full participation even by those present may be inhibited. Professional studies have indicated that human behavior can be inhibited simply by the sense of being placed under scrutiny;[188] FBI officials themselves appear to have recognized the existence of such a chilling effect.[189] Although privacy interests per se were rejected as a rationale for restricting informers in *Hoffa*[190] and *White*,[191] the first amendment ramifications of invasion of privacy were not explored in the prevailing opinions.[192]

2. *Control of Informers.* — Given the potential of the use of informers to chill political activity, their employment in pursuit of legitimate objectives should be so constrained as to inflict the minimum possible harm on first amendment interests, or at least so constrained that the degree of their use reflects a balance between proper government objectives and guaranteed political freedoms.[193] The proper ultimate objectives for the use of informers would seem, of course, to be the prevention and detection of crime. Those interests are particularly strong when the crimes in question create national security risks — as may crimes such as sabotage, assassination, and inciting or instigating widespread civil disorder[194] — and are totally absent with

[187] Fried, *Privacy*, 77 YALE L.J. 475, 482–83 (1968).

[188] A. WESTIN, PRIVACY AND FREEDOM 58 (1967); works cited *id.* at 403 n.14.

[189] One of the Media Papers contained a suggestion by the Philadelphia office of the FBI that there be more investigations of New Left groups in order to "enhance the paranoia endemic in these circles and [to] further serve to get the point across that there is an FBI agent behind every mailbox." N.Y. Times, March 25, 1971, at 33, col. 1.

[190] Hoffa v. United States, 385 U.S. 293 (1966).

[191] United States v. White, 401 U.S. 745 (1971).

[192] *But see id.* at 787–88 (Harlan, J., dissenting) (use of wired informants will chill discourse).

[193] *Cf.* pp. 1170–73 *supra*.

[194] In authorizing wiretapping solely for national security purposes, President

regard to political activity protected by the Constitution or outside legislative proscription. Nevertheless, those interests may be used to justify infiltration of almost any dissident political organization. Any opponent of government policies might become a violent opponent. Thus, informers are employed for the ongoing collection of general intelligence about the activities and plans of organizations and individuals who oppose the Government's policies and who are perceived by officials as capable of endangering the national security. There is evidence to indicate that a substantial amount of the surveillance by informers directed by the FBI can be described as having this intelligence purpose.[105] Particularly in recent years, the Government has tried to remain aware of the activities of dissident black and antiwar groups, even though there may be little to connect the particular groups closely to the anticipated commission of criminal acts.[106] Such intelligence quite possibly facilitates appropriate government responses in case violence or disorder does occur. That advantage must, however, be weighed against the danger of chilling protected political activity.

It might be argued in response that no explicit constitutional standard is necessary, since it is in the interest of the police to employ informers efficiently — only when they are likely to provide useful information related to criminal activity. But there are several reasons why police agencies may tend to overuse this technique. First, the intrinsic unreliability of informers themselves may engender their excessive utilization. An informer may exaggerate his reports because of a sense that his remuneration and employment are dependent on the incriminating nature of

---

Roosevelt noted: "It is too late to do anything about it after sabotage, assassination and 'fifth column' activities are completed." Roosevelt Memorandum 670.

[105] The widespread gathering of information to facilitate presidential decision-making in situations which might call for the use of federal troops would fall within the intelligence purpose. *Constitutional Rights Hearings*, pt. 1, at 500, 912. One commentator asserts that most FBI informers are used for the gathering of political intelligence. F. Donner, The FBI Informer — His Role in the American Political Intelligence System 1, Oct. 29, 1971 (unpublished paper delivered at conference on the FBI sponsored by the Committee for Public Justice; on file at the *Harvard Law Review*).

[106] In one of the Media Papers, FBI Director Hoover requested an increase in the "quality and quantity of intelligence information on Black Student Unions." N.Y. Times, March 25, 1971, at 33, col. 1. Since the request was based on the student groups being potential targets of influence for the Black Panthers rather than on any connection between the groups and the commission of any criminal offense, *id.*, such a request would seem to have been directed far more to an intelligence purpose than a crime prevention purpose. Additionally, an eleven-page FBI report on Earth Day activities seemed not to be related to the expected commission of any crime. NEWSWEEK, April 26, 1971, at 23.

the information which he delivers,[197] or he may even be impelled by ulterior motives such as revenge. If police agencies are not extraordinarily careful to check the reliability of their informers,[198] then informers who manufacture incriminating data may be rewarded or retained for the infiltration of truly harmless or even constructive organizations.

A second likely reason for excessive use of informers is bureaucratic. A government bureau with the mission to conduct surveillance and collect information has a vested interest in the continuation and expansion of such functions.[199] As perceived by the FBI, one index of the success of its performance is the quantity [200] and precision [201] of the information that it has gathered. What is more, the effectiveness of an individual agent is measured in part by the quantity and quality of data that his investigations provide, thus giving agents a personal incentive to maximize the amount of information that they generate.[202]

The final likely reason for overuse of informers is one characteristic of the national security area and one which may have particular force with regard to police agencies. The executive has a strong tendency to exaggerate the dangers of political dissent.[203] The use of informers to infiltrate a particular organization may therefore reflect solely the degree of that organization's disagreement with government policies. Not only may such infiltration be designed to uncover specific violent activities or plans; it also may be designed simply to inhibit the growth of the infiltrated group. Although there is little evidence of such a conscious purpose at high echelons of the Government,

---

[197] F. Donner, *supra* note 195, at 44.

[198] One method used by the FBI to assure the reliability of their informers is to assign two informers to report on a single event or organization and to compare the information that each delivers. Wall Interview, *supra* note 181.

[199] *See* R. Longaker, The Presidency and Individual Liberties 5–6 (1961). For a discussion of some factors which may intensify the tendency of an organization to pursue rather narrow vested interests, see G. Allison, Essence of Decision: Explaining the Cuban Missile Crisis 81–83 (1971). In the governmental area, of course, expansion of function may lead to increased funding.

[200] For example, J. Edgar Hoover has testified that "A total of 7,220,816 sets of fingerprints were received for processing [by the FBI] during the fiscal year 1970, representing a daily average of 28,768 sets of prints." *Hearings on Dep'ts of State, Justice, and Commerce, the Judiciary, and Related Agencies Appropriations for 1972 Before a Subcomm. of the House Comm. on Appropriations*, 92d Cong., 1st Sess., pt. 1, at 694 (1971).

[201] For instance, Hoover testified in 1955 that there were "approximately" 22,263 Communists in the United States. *Hearings on Dep'ts of State and Justice, the Judiciary, and Related Agencies Appropriations for 1956 Before a Subcomm. of the House Comm. on Appropriations*, 84th Cong., 1st Sess. 167 (1955).

[202] Wall Interview, *supra* note 181.

[203] *See* Section II *supra*.

there are indications that, at least at some lower levels, the regularized surveillance and collection of information on political groups is intended to discourage political activity.[204]

While all these considerations suggest that police agencies in particular, and the executive in general, cannot be relied upon to accommodate the need of informers and first amendment interests on their own initiative, still any balance to be effectively struck between the two sets of interests will need to be enforced by the executive itself. The courts, and even the legislature, are not well equipped to control the use of informers. It is difficult to judge with confidence the motive behind a particular infiltration by an informer; real but peripheral expectations of crime could be cited to support surveillance politically motivated at root. For example, a law enforcement agency could justify infiltration of many dissident political groups as an attempt to uncover information relating to drug violations.

In addition, a number of institutional constraints limit the potential of the courts in particular to eliminate abusive government infiltration. First, the Supreme Court is unlikely to require prior judicial approval for each use of informers. The first amendment, in contrast to the fourth, requires no such advance sanction of each government action arguably offensive to its mandates. Since the Court's refusal in *Hoffa* to impose a prior-approval standard on the broad range of informer cases through the fourth amendment [205] surely reflected an appreciation of the usefulness of informers in law enforcement, the Court is hardly likely now to lay down the same requirement through a constitutional provision that makes no mention of that standard. The requirement would likely be incapable of enforcement anyway. The use of informers is extremely widespread,[206] and the decision for their deployment in each case (at least within the FBI) is gen-

---

[204] *See* note 189 *supra*. One commentator argues that "the recruitment of informers is *intended* as a restraint on free expression." F. Donner, *supra* note 195, at 14 (emphasis in original). A former FBI agent has alleged that agents have forged letters in attempting to foment dissent among antiwar groups. Wall, *supra* note 155, at 14–15. He also alleges that, to minimize the size of demonstrations, the FBI distributed leaflets containing erroneous information about the time and place of the demonstrations. *Id.* at 14. Although conceding that individual agents may have engaged in such activities, former Attorney General Mitchell has denied the existence of a domestic counter-intelligence program in the Bureau. Televised interview on *Today*, Jan. 27, 1972.

[205] *See* pp. 1273–74 *supra*.

[206] Indeed, it may be, since overt surveillance might require a larger commitment of a law enforcement agent's time and energy than the use of an informer, that the latter technique is sometimes employed in preference to the former. *See* Wall, *supra* note 155, at 14. The recruitment of informers is a central task of many FBI agents. F. Donner, *supra* note 195, at 21.

erally made at a low level in the bureaucratic hierarchy.[207] It may be made rapidly, and it is certainly made informally, perhaps as an opportunity presents itself.

Finally, the most important reason that a prior-approval requirement might prove incapable of enforcement overlaps with a second set of reasons that any judicially enforced substantive standard for the use of informers — with or without a prior-approval restriction — is likely to be impracticable. The police would suffer no adverse consequences from failure to comply with either a warrant requirement *or* a substantive criterion. Suits for injunctive relief or damages[208] as a result of improper use of informers may well fail because of difficulty in marshalling facts to prove infiltration.[209] Also, any use of a first amendment "exclusionary rule" in criminal prosecutions is unlikely to have a significant impact on the practice. In precisely the least justified instances of the use of informers, an informer may be collecting only intelligence information with no prosecutions in sight; and when there are criminal trials, it may be practically impossible — in contrast to the situation with national security electronic surveillance — to determine if the defendant has been observed or overheard by any one of very many informers retained informally by lower echelon law enforcement officers.

Despite all these considerations, the judiciary, or even the legislature, could play some role in controlling abusive use of informers by the executive. If the judiciary or Congress could once articulate a general standard for the use of informers, then it could require the executive in the first instance to implement that standard through the promulgation of more specific, formal regulations.[210] At present, there are no published regulations cover-

[207] Wall Interview, *supra* note 181. The low level at which informers are authorized to be used stands in rather stark contrast to the situation with regard to electronic surveillance. Under the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2516(1) (1970), it is only the Attorney General and designated Assistant Attorneys General within the federal government who can authorize an application for a wiretapping warrant.

[208] In a fourth amendment context the Supreme Court has held that violation of an individual's constitutional rights by federal agents is in itself grounds to hold the agents personally liable in damages. Bivens v. Six Unknown Named Agents of the Bureau of Narcotics, 403 U.S. 388 (1971).

[209] For example, in Turco v. Allen, 334 F. Supp. 209 (D. Md. 1971), the Black Panther Party sought an injunction against state law enforcement officials infiltrating the organization, but relief was denied partially for want of factual allegations supporting the claim. *Id.* at 218.

[210] A court might issue an injunction allowing the executive and or legislature a specified period of time to promulgate and publish acceptable rules to clarify the bounds of investigative discretion in the use of informers. *See* United States v. Bryant, 439 F.2d 642, 652 (D.C. Cir. 1971). *See generally* Sedler, *Conditional, Experimental, and Substitutional Relief*, 16 RUTGERS L. REV. 639, 716–27 (1962).

ing the criteria to be used by federal investigative agencies in deciding whether or not to employ an informer in a given situation.[211] Publication of standards would ease the task of an agent's superiors or the courts in determining the true motive behind a particular infiltration; for example, if an informer is claimed to be investigating drug traffic, rather than political activity, the agent would have to show that the prerequisites for infiltrating drug activity had been satisfied. Publication of standards by the executive would also help inform the other two branches of current practice, facilitating the construction of further controls. Finally, and perhaps most importantly, published regulations might change public perceptions of law enforcement practice. Even if agency actions are conducted circumspectly without published regulations, the lack of standards can result in public belief that the agency is acting far beyond the bounds of propriety. In terms of a chilling effect on political activity, this perception of the agency may be as important as the agency's actual behavior.

The problem for court or legislature — or for that matter for a conscientious executive — is therefore to articulate a substantive standard for the use of informers that takes account both of law enforcement needs and of political liberties protected by the first amendment. In areas other than the use of informers, the governmental tendency to intrude too far into political activity in the name of national security has been checked by forbidding government intrusion unless the political activity can be tied quite directly to unlawful conduct. Speech cannot be prohibited unless the danger of unlawful conduct is "imminent."[212] Membership in an organization cannot be a cause for criminal sanctions unless the organization has an unlawful purpose, the member intends to further that purpose, and the member is active in the organization. The same standard generally applies when membership is penalized by denial of a job or passport.[213]

Admittedly, a less immediate tie to illegal conduct may be called for to justify the use of informers, both because infiltration is not itself a sanction and because the very purpose of informers is to discover the likelihood of unlawful action. An informer's potential value is indeed diminished if he can be employed only once some information on impending illegal activity is available.

---

[211] Assistant Attorney General Mardian has testified that the FBI's "guidelines with respect to investigation of crimes, including civil disorders, have not been published." *Constitutional Rights Hearings*, pt. 1, at 871.

[212] Brandenburg v. Ohio, 395 U.S. 444 (1969); *see* p. 1137 *supra*.

[213] United States v. Robel 389 U.S. 258 (1967). Only in the case of highly sensitive positions might it be desirable to deny employment to individuals on the basis of only "knowing membership" in organizations which have an unlawful purpose. *See* pp. 1174–76 *supra*.

Nevertheless, infiltration of political organizations by informers should not be permitted unless there is at least a reasonable expectation that their use will reveal information relating to the commission of a criminal offense. The fact that infiltration is not itself a sanction does not negate its capacity to chill association — or even to be used intentionally with that effect. And if, therefore, by analogy to other "chilling" problems, at least some tie to criminal conduct is to be required to justify a government intrusion,[214] it is difficult to see how any standard less than "reasonable expectation" could have any restraining effect at all.

A reasonable expectation standard would prohibit the introduction of informers into a group solely because of the political views of its members — either with the hope of discovering criminal activity or with actual intent to discourage membership activities — and it would require that infiltration be discontinued if information concerning crime did not appear after a reasonable length of time.[215] Its chief costs to the Government probably would concern the governmental interest in having as much information as possible in order to be maximally prepared for civil disorder. But reasonable use of informers would still be permitted; and preparing for civil disorder can be accomplished in part by alternative means. The public media can be scrutinized for intelligence information. Extra law enforcement officials can be held on call during demonstrations that present even a small possibility of civil disorder. And, of course, the police can openly maintain contact with groups or communities where disorder may appear.[216]

Perhaps the most serious criticism of a reasonable expectation standard must come from the other side. As we have already suggested with regard to any standard less stringent than

---

[214] The absence of a nexus between "the information sought and a subject of overriding and compelling state interest," Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539, 546 (1963), has been found to invalidate a legislative investigation when that investigation intrudes "into constitutionally protected rights of speech, press, association, and petition." *Id.* *See also* Sweezy v. New Hampshire, 354 U.S. 234, 251 (1957).

[215] One commentator indicates that "even if a preliminary [FBI] probe produces negative results, the informer is told to continue his undercover activity." F. Donner, *supra* note 195, at 19. A former agent noted that because of bureaucratic factors, investigatory files tend to remain open for inordinately long periods of time, creating a situation in which "the investigations of hundreds of perfectly harmless people continued on through the years." Wall, *supra* note 155, at 14.

[216] It should be noted, however, that with the exception of the privacy interest in avoiding surveillance per se, the first amendment "chilling effect" interests affected by the intensive surveillance of and detailed data collection on public political activities are similar to those affected by the use of informers. *See* pp. 1274–76 *supra*.

reasonable expectation, the criterion may degenerate into no requirement at all. A partial answer might be for the judiciary or the legislature to regulate more strictly the use and dissemination (or even storage) of informer-supplied data. In particular, to prevent the misuse of information about a person's protected speech and association, the courts, both as a matter of first amendment adjudication and pursuant to statute, can review the substantive basis of governmental actions such as denial of employment,[217] and can limit both the storage of information and the dissemination of data to inappropriate individuals and institutions.[218] Infiltration by informers might not be reduced by such controls, but the resulting chill on political activity would probably diminish as the public gained confidence that the use of informers would not lead to injury to an individual on the basis of protected speech or association. Moreover, such assurance would operate as well to reduce the chilling effects of intensive government surveillance of public political activities — chilling effects that take on great force from the possibilities of excessive collection, indiscriminate dissemination, and invidious use of data about an individual citizen's political activities.[219]

---

[217] *See* Kahn v. Secretary of Health, Educ., & Welfare, 53 F.R.D. 241 (D. Mass. 1971); pp. 1183–84 *supra*. It may be that, even if the FBI would find it impractical to deploy an informer for purposes of an individual loyalty investigation, information collected by previous informers could be most useful in security checks.

[218] *See* Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971). Congressional hearings have been held to search for appropriate means of control. *See, e.g.*, *Constitutional Rights Hearings*. One common suggestion is that information gathered through surveillance should be stored only so long as it serves the valid purpose for which it was collected. Countryman, *The Diminishing Right of Privacy: The Personal Dossier and the Computer*, 49 TEXAS L. REV. 837, 869 (1971). The termination of a crime-related investigation, for example, should perhaps be accompanied by an expungement of names and information gathered in that investigation which have turned out to be unrelated to the commission of any crime. *Id.*

[219] *See* note 216 *supra*.

BUT SO IS THE RIGHT TO LAW AND ORDER

By Clarence D. Kelley

One of the most studied problems in American society today is that of the invasion of the right of privacy. Stories abound on the subject in the news media. Jurists debate the various legal questions associated with this complex issue. Both chambers of Congress have formed committees to explore constitutional rights, focusing on privacy. In addition, the President in early 1974 established the Domestic Council Committee on the Right of Privacy. Since each of us cherishes his privacy, the extensive study being afforded this issue is certainly merited.

When considering the issue of the right of privacy, it is particularly important to be reminded that this is not a new idea. In fact, this right lies at the roots of our American heritage. Incensed reaction to the continuous infringement on the personal liberty of our early colonists gave birth to this Nation — and it has been the protection of our hard-won rights that has sustained our Republic through nearly two centuries.

Freedom, of course, is what America is all about. However, to guarantee tranquility for all, freedom must be regulated. Total freedom would be chaotic. Therefore, for the good of all, rules must be established and laws must be enforced. It is in this area of maintaining the peace that problems have arisen regarding the methods of enforcing the law and concerning the retention of criminal records. At the core of the problems lies the issue of the right of privacy.

Clarence D. Kelley is the Director of the Federal Bureau of Investigation

Interestingly enough, this right is not defined nor specified in our Constitution. Yet, the principle of privacy permeates this document. Though privacy is not specifically mentioned, it is certainly a factor in the First Amendment (religion, speech, press, assembly), Third Amendment (quartering troops), Fourth Amendment (unreasonable search and seizure), Fifth Amendment (self-incrimination), and Ninth Amendment (rights enumerated in the Constitution not to be construed to deny or disparage others retained by the people). Therefore, to paraphrase my earlier statement, privacy is what freedom is all about.

In its more than 60 years of operation, the Federal Bureau of Investigation (FBI) has been acutely attuned to protecting individual rights and liberties. The right of privacy is — and has been — of importance to the FBI in all of its activities. For instance, FBI records contain a vast amount of information which, if improperly maintained and disseminated, could be the cause for genuine concern by those most interested in the right of privacy. Fully realizing this, the FBI remains keenly aware of the necessity to safeguard the data entrusted to our organization. In addition to protecting the privacy of persons by imposing strict controls over accumulated data, the FBI also confronts the issue in certain phases of its investigative efforts. The right of privacy is one of the factors concerning how penetrating an FBI investigation can be and to whom the results can subsequently be reported.

INFORMATION SYSTEMS

Criminal justice information systems are the target of those most concerned about the possibility of the invasion of privacy. Criticism is leveled at the types of information stored in the systems, the validity of the data, the necessity for the information, the dissemination of the material, and the eventual purging or retention of the information. While

(continued on page 27)

Kelley from page 23

it is true that the majority of the records of the criminal justice profession are maintained in manual systems, it is also a well-known fact that computerized systems are being increasingly implemented at all levels of the profession. It is this spreading computerization, with its ability to provide rapid access to large amounts of information, that has produced most of the concern for individual privacy.

I believe that a look at the file structure of the FBI can provide an understanding of how the privacy issue affects the FBI and the rest of the criminal justice profession. The FBI maintains three basic categories of records: FBI Identification Records, investigative files, and the National Crime Information Center (NCIC).

When a person is arrested by local, state, or federal law enforcement agencies, fingerprints and arrest data are forwarded to the FBI, which uses this information to compile the person's Identification Record. Such arrest records (sometimes referred to as "rap sheets") may later be used in identifying suspects, in locating fugitives, and in providing guidance in bail, sentencing, and probation matters.

While Identification Records do provide a valuable service to law enforcement, one problem exists: to be complete, the record must reflect the eventual disposition of the charges against the persons arrested. While arrest information is usually immediately provided to the FBI, the data concerning final disposition is much more slowly furnished — if at all. To minimize inequities that can arise when Identification Records are used for non-law enforcement purposes, the FBI adopted a policy as of July 1, 1974, regarding the processing of these civil-type fingerprints.

We have discontinued furnishing the inquiring agency any information regarding arrests that are more than one year old *unless* the disposition of that arrest is also shown on the individual's Identification Record.

Citizens should also feel encouraged to learn that since 1973 any person can request a copy of his own Identification Record. If he then questions the accuracy or the completeness of any entry on that arrest record, he can arrange for it to be amended by the law enforcement agency which furnished the original data.

The investigative files of the FBI contain the results of our investigations into matters within our jurisdiction. These files are composed almost entirely of interviews of citizens, officials, and informants. Legislation is presently being proposed which would allow individuals to personally review FBI investigative files concerning them, to determine the accuracy of the information and request correction of any errors. While those advocating such legislation have the highest ideals, it would be virtually impossible for the FBI to function satisfactorily if subjects of investigative files are permitted to inspect their files. Persons, including informants, would no longer willingly provide information for fear their identity would be learned. In some instances, due to the serious nature of the case, the lives of individuals would be at stake.

NATIONAL CRIME INFORMATION CENTER

The third basic category of files maintained by the FBI is the NCIC, which is a computerized index of stolen property, wanted persons, and criminal histories. The system is an excellent example of how modern technology has been effectively and responsibly employed by law enforcement. Although only operational since 1967, NCIC has become one of the most potent weapons against lawlessness.

NCIC was developed with a full recognition of the necessity to properly regulate and control it. Today this computerized information system, operated under strict professional management and careful safeguards, serves the cause of better law enforcement with distinction and without abuse of privacy rights.

Despite its lengthy record of success, NCIC has received some criticism, the bulk of which has been aimed at the computerized criminal histories portion of the system. I believe the criticism is occasioned because the purpose of these histories is misunderstood. Their sole purpose is to speed up the criminal justice process by making needed information rapidly available.

In appearances before Congress and the public at large during the past several months, I have endeavored to point out the vital function of criminal justice information systems in maintaining a free and just society. I have stressed insuring that appropriate controls are established to guarantee that the information in these record systems is not misused, that the right of privacy is protected.

LAW ENFORCEMENT AND PRIVACY LEGISLATION

On March 7, I testified before the US Senate's Judiciary Subcommittee on Constitutional Rights relative to a number of proposed privacy bills. The ultimate aims of the bills that I discussed were to protect the individual against improper use of information collected by criminal justice agencies, and I am wholly in accord with this basic intent. Together with all responsible members of the law enforcement profession, I welcome the creation of legal sanctions against misuse of criminal justice information. We are acutely aware that misuse of such data may be extremely injurious to an individual's reputation and welfare.

While I emphasized to Congress my support of the formalization and clarification of controls on criminal justice information systems, I also took the occasion to point out that certain aspects of the legislation under consideration did not appear to be in the best interests of law enforcement and society as a whole. I felt then, as I do now, that our zeal to protect individual privacy must be tempered with a concern for an effective system of criminal justice.

In respect to key issues raised by these privacy bills, I have opposed provisions calling for the purging of conviction records. There are, I believe, substantial reasons for preserving this information. For example, under these provisions, fingerprint records would be unavailable for future comparison purposes, and records of prior criminal activity would be unavailable for sentencing purposes.

It is my belief, too, that a criminal justice information system should be controlled and operated by a criminal justice agency and should not share equipment, facilities,

(continued on page 32)

Kelley from page 2

gr procedures with any noncriminal justice system in order to insure the security of the information and to protect the privacy of individuals about whom the information applies.

Furthermore, I am opposed to inclusion of criminal intelligence information in systems to which direct, unchecked access is given to other agencies, even other criminal justice agencies, unless appropriate safeguards have been provided. The unverified nature of much intelligence information, as well as its sensitivity, particularly from the standpoint of protecting the source, calls for restricted handling.

I have also questioned the wisdom of flatly denying criminal offender information to noncriminal justice agencies where there exist legitimate needs for this data, such as in determining access to classified and sensitive information or in determining suitability for federal employment.

Another key issue involves the sealing of records. Proponents of such a restriction would have criminal offender record information, such as fingerprint cards and "rap sheets," sealed after a stipulated period of time and thus unavailable for use by even criminal justice agencies. The stated purpose of sealing is to prevent an individual's record from adversely affecting him in later years, possibly after rehabilitation. It is, however, my view that sealing against criminal justice agencies is unwarranted and would act as a serious investigative handicap. I am convinced that the investigative value of such records, when confined within criminal justice agencies, far outweighs the relatively small possibility of their misuse.

I also expressed to the Subcommittee my deep concern over proposals to impose on criminal justice agencies blanket prohibitions against using such modern technological advances as the computer. This sort of arbitrary restriction on progress makes little sense to me. Control — not denial — is the proper approach to the utilization of modern technology.

THE NEEDS OF SOCIETY VS. THE NEEDS OF THE INDIVIDUAL

Before closing this discussion, we would do well to take an overall view of the situation. We must look at the best interests of *both* society and the individual.

The right of privacy does not mean that shackles must be thrown around the legitimate operations of the law enforcement officer. It also does not mean that a citizen can freely declare that his activities are free from scrutiny. No person in our society is above the law.

Historically, in America freedom has meant a balance of individual and societal rights. Never is it a question of one or the other, but both. The moment we lose this balance, our free society will be jeopardized.

Any criminal justice information system must give *equal* concern to protecting the rights of all individuals and to the necessity for law enforcement agencies to have all pertinent information to meet their responsibilities. This represents quite a delicate balance, but a balance that has to be maintained.

Just as each of us treasures his personal privacy, it is our obligation to respect the privacy of others. Likewise, because of our professional responsibilities, it is essential that we have access to all information that will aid us in providing criminal justice. The challenge of combating crime while giving utmost concern to personal privacy is certainly complex, but it is a challenge that must be successfully handled for the good of all.

TRIAL Magazine

Center Report, v. IX, Apr. 1976

Herbert Scoville, Jr.

IS ESPIONAGE A NECESSARY INSTRUMENT FOR INTELLIGENCE GATHERING?

The following paper by Herbert Scoville, Jr., was given at a recent conference on Controlling the Intelligence Agencies, convened by the Center for National Security Studies and Civil Liberties, a Fund for Peace affiliate, with which the Center for the Study of Democratic Institutions maintains an informal relationship. Scoville has had a long career in national security matters. He was one of the first officials of the Armed Forces Special Weapons Project, an agency created in the Defense Department at the end of World War II, after the termination of the Manhattan Project, to sponsor and conduct research on nuclear weapons effects. Later he was Deputy Director for Science and Technology at the CIA and subsequently with the U.S. Arms Control & Disarmament Agency as Associate Director for Science and Technology. He is presently Secretary of the Federation of American Scientists.

The value of human covert intelligence sources has, in recent years, come into increasing question as the capabilities of technical methods have become more and more all-encompassing and sophisticated, and as the political liabilities of human covert operations become increasingly evident. Too often extreme points of view have been taken, as on one side it has become popular in this country to condemn all covert operations, and, on the other, for the intelligent traditionalists to nostalgically defend the experiences of the past. In my view, it would be extreme madness to say that espionage is completely unnecessary and not a useful intelligence tool. Even if it never produced any useful information, the existence of a covert collection capability has value, since leaders in other nations can never be certain that their plans will go undetected. On the other hand, it would be equally foolish not to recognize the severe limitations of such sources and, therefore, not to minimize reliance on covert operations.

I shall first attempt to describe briefly the major alternative sources of intelligence information, to evaluate their usefulness and limitations in providing for our major intelligence requirements. Then it will be possible to analyze how espionage can realistically be expected to supplement these sources so that one can determine how necessary it really is and what scale of covert operations the U.S. Government needs. These needs must then, of course, be balanced against the political risks that such operations entail.

Intelligence collection can be roughly broken down into four major categories: overhead photographic observation primarily from satellites, communications and other electronic intelligence, open literature, and covert human sources, i.e., agents and defectors. The major intelligence targets can be separated into three general groups: military information on the forces, weapons and plans of our potential foes; political intelligence on the make-up, intentions, and interrelations of individuals and organizations in and out of foreign governments, and finally economic intelligence on the resources, technology, and fiscal health of all countries. Of course, these areas cannot be clearly delineated since, for example, military and political intentions are strongly interconnected and economic factors will have a profound influence on both these areas. However, they do provide useful categories for analyzing the effectiveness of various intelligence sources.

In the military area, there is little question that photo-intelligence provides not only the greatest quantity but also the highest quality information. Satellite photography, unlike aircraft reconnaissance can, in a relatively short period of time, provide visual evidence of military deployments throughout very large areas. Moderate resolution photography can be used to provide almost continuous surveillance of a country even as large as the Soviet Union, and high resolution systems can provide detailed information on targets of specific interest. The greatest drawback in this area is cloud cover, but almost all areas of the world are subject to overhead photography without prolonged delay. Relying on cloud cover to conceal operations is a risky tactic. Of course, a camera cannot see through the roofs of a building, but with modern military technology it is hard to keep any significant weapons program or troop deployment completely concealed from the camera's eyes. The construction of new facilities, the shapes of buildings, and the required logistic support almost inevitably provide clues as to the existence and nature of a military target. Road patterns and excavations give evidence of missile sites long before they become operational.

The main exception is the ocean: photography, even using sophisticated infrared techniques, is not capable of making observations below the surface of the water. Therefore, it is not useful for locating submerged submarines at sea, but such ships are observable in their home ports and during construction. Acoustic sensors on ships or on the sea floor must be used in place of cameras to maintain surveillance of submarines under water.

Communications and other electronic intelligence are also an extremely valuable source of information in the military area. These provide very extensive data on the characteristics of weapons as they are being developed and tested, on their deployment, and in many cases on plans for their use. Communications security, through the use of codes and other techniques, can decrease the reliability of these sources, but it is not always practical to use such counter-measures on the scale needed to conceal modern military operations. Opportunities for mistakes are manifold. Conversely, however, too heavy reliance on such techniques can lead to grievous intelligence failures. A good example is the recently publicized misinterpretation of our com-

munication intelligence before the outbreak of the October, 1973 Middle Eastern conflict.

Such intelligence, of course, is not limited purely to monitoring communications. Most modern military systems make extensive use of radars, and the ability to record the emanations from such equipment is an important intelligence asset. An air defense radar which is not in operation and therefore potentially monitorable provides little air defense. The nature of the radio waves from electronic equipment provides a clever analyst clues for determining the characteristics and the capabilities of the radar. Spoofing this type of intelligence is not easy since radars must be operated properly to be effective.

While open literature on U.S. military matters is undoubtedly a valuable resource for foreign intelligence organizations, it has relatively limited value for the U.S., at least for providing information on the military capabilities of the U.S.S.R. and China. They do not have a parallel to *Aviation Week* or the Congressional hearings. Even the military literature that does fall into our hands is often suspect. Those who are allowed to publish in the Soviet Union rarely express the inner thinking of the influential Soviet military planners. Sometimes, such articles express the wishes of military minds but bear little resemblance to real policies. Often, they are put out to serve political objectives and are therefore untrustworthy. In many cases, they are simply mirroring U.S. thinking in order to make up for their inability to publish Soviet views. Technical literature almost never contains any material of real military interest and too often intelligence analysts are left to draw conclusions from what is not published rather than from what is.

Human covert sources rarely provide useful intelligence in the military area. It is hard enough to recruit an agent who has any inside knowledge on military affairs, but it is even more difficult to recruit one who has sufficient technical background to provide timely and meaningful information on the characteristics of modern weapons. Even Penkovsky, the most celebrated Western spy, provided in retrospect little information of major importance. Since such sources were extremely rare and usually nonexistent, every little tidbit that he provided was gobbled up with great avidity by the intelligence community, but now more than fifteen years later, it is hard to recollect any specific information which had a significant effect on our intelligence estimates. And this was at a period when our technical means of collection were far inferior to what they are today. While another Penkovsky may be developed in the future, it is clearly difficult to see how such agents can ever be a major factor in our intelligence on Soviet or Chinese military matters. In other countries, where security is less stringent, they could be of somewhat greater value.

"Human covert sources rarely provide useful military intelligence."

Only in the area of military intentions can espionage be anticipated to play an important role, but even here, it is my view that the potentialities are often greatly exaggerated. It would be extremely fortuitous if an agent could be recruited to provide advance information of an impending military operation. A defector might, by chance, supply some facts, but the time delay in getting his knowledge to the intelligence community would normally be too long to permit appropriate counteraction. Furthermore, the very nature of such sources renders them very unreliable in time of crisis. Agents are too often doubled or suspect for personality reasons. It seems likely that unless the information could be confirmed by other means, it might well be ignored. For example, at the time of the Cuban missile crisis, there were reports from sixty-four sources that missiles were in Cuba. Many of these were patently false, partly because of the confusion between offensive and defensive missiles, which were known to be in the process of deployment. In a post mortem after the crisis was over, it was determined that only six of these reports were accurate, but the value of the information from these human sources was lost in the noise of the inaccurate information.

Meanwhile, the value of other intelligence sources in the intentions area cannot be completely discounted. Photographic information on the location of deployed forces, their movements and their capabilities gives clues as to their probable plans for use. Communications and electronic intelligence can be of even more direct value although quite susceptible to deception. Even open sources can be occasionally of value; as, for example, the acquisition of the advance Soviet press release, which provided President Kennedy with three days' notice that the Soviet Union was intending to abrogate a nuclear test moratorium in 1961.

In the economic area espionage has probably even relatively less value. Economic information by its very nature tends to be more openly available even behind the iron and bamboo curtains. Economic information must be more broadly disseminated than military, since it is necessary for the normal operation of the government. This is particularly true in such nations as U.S.S.R. with its highly centralized economic planning. There are many non-classified sources of information to assist the economic intelligence analyst. Even photography can be useful as has been shown by the advance information reported to have been available on Soviet crop failures. It is probably rarely necessary or desirable to employ a recruited agent to supply economic information, but occasionally defectors or overt human sources undoubtedly provide useful information in this area.

In the political intelligence field, however, espionage probably finds its greatest justification. Here, one is seeking to understand what is going on in the minds of men. This is not susceptible to technological intelligence collection. When such ideas are

translated into words or put on paper, the opportunities for procuring the information by espionage increases. The theft of a plan is always a distinct possibility, but the difficulties in carrying out such a covert operation are extraordinarily great. Bugging the Kremlin is a nice idea for spy fiction, but our national security planners had better not place any reliance on such a source. Recruiting an agent who is privy to the inner Soviet circles can be an important goal of our clandestine services but it is not to be counted on. Monitoring of communications has probably a greater chance of success in the sensitive political arena, but even such methods are very unreliable because of the ease in providing communications security over important political matters. As the information radiates out from the centers of the Communist world to the satellites and to Communist groups overseas, the opportunities for obtaining information through agents, defectors, or communications increases, but simultaneously the importance of the information decreases.

It is only when one gets out into the Third World that the opportunities for agent collection become really significant. Security in many of these nations is much more haphazard; availability of agents very much greater. In many countries, governments come and go with extraordinary rapidity; thus creating large numbers of dissident or dissatisfied individuals with access to inside Information. Understanding of the political motivations and advance knowledge of the plans of all elements in a country is, of course, an important intelligence objective. This can sometimes be obtained through overt liaison and normal diplomatic channels. Open press and literature sources are also useful, but unquestionably, in some cases covert relationships provide a valuable source of information. This could be particularly critical in the case of terrorist or dissident groups that might be considering nuclear blackmail. However, an agent can also frequently be an important source of misinformation since he may often have ulterior motives in supplying intelligence. This can be particularly true in cases

"We have no room for operations for operations' sake..."

where covert action, such as the overthrow of the government, is also involved. This is another reason why such covert actions should be abandoned or at least divorced from intelligence collection.

Even in the case of highly secure societies, public information and overt means are probably the most important sources of political intelligence. Over the years, there have developed a coterie of experts on Soviet society and politics. Similar groups, although far less extensive, follow other areas of the world. The intelligence community has it own inside experts who have access to classified information as well as public. Undoubtedly, information obtained by espionage provides a small but occasionally high-quality addition to the more readily available data. The availability of classified sources to check what is openly available is always useful to avoid being misled, but agents are not necessarily the most readily available or even the most reliable sources for this purpose.

Open sources of information are attractive because their collection involves no political drawbacks and their use can almost always be publicized without compromising the future intelligence capabilities. Although overhead photography initially involved very sensitive operations because of the need for illegal overflights — such as the U-2 — these no longer do so now that satellite platforms can be used. Although still shrouded in security, satellite photography has been given international legal status by the Soviet Union when, in the ABM Treaty, it formally recognized that such means of intelligence collection were essential to the verification of that Treaty. Communications and other electronic intelligence collection is generally accepted as a fact of life throughout the world even though it does have questionable legal authority. In most cases, such information can be obtained without necessity for conducting clandestine operations in a target country. However, because in the communications area, success is very dependent on the degree of communication security, the information obtained normally has to be highly classified in order to prevent compromise of future operations. This does decrease the usefulness of the source. Agent operations suffer from the dual drawback of being illegal, thus involving potential political repercussions, and being subject to compromise if disclosed. Therefore, information from such sources is much more difficult to use than that from the others.

In sum, espionage would appear to have only limited potential as a source of intelligence information. In the national security and military areas, it rarely will supply data of any great value and is a relatively unimportant and less reliable adjunct to technological methods. These latter probably are more useful even in providing the basis for determining the intentions of Soviet and Chinese leaders than espionage. Open published information and that obtained through diplomatic and other overt contacts is far and wide the most generally useful source of political and economic intelligence. Nevertheless, it would be wrong in my view to halt all clandestine agent operations for the collection of intelligence. These can be most useful, not in the U.S.S.R. and China where security and control over individuals is great, but in nations where the knowledge of the attitudes of persons outside, as well as inside the government, is essential if we are to conduct a sound foreign policy. However, the limited value of agent operations combined with their potential political liabilities makes it incumbent on the government to limit such activities to those areas where the potential gains clearly outweigh the potential risks. We have no room for operations for operations' sake in our intelligence structure. ■

79-064 O - 76 - 44

(Article by Thomas I. Sheridan

from the Fordham Law Review)

NOTES

ELECTRONIC INTELLIGENCE GATHERING AND THE OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968

I. Introduction

In *Berger v. New York*[1] the Supreme Court reversed a bribery conspiracy conviction that was based on evidence obtained by means of a court authorized "bug"[2] installed in the defendant's office pursuant to a state statute. In *Katz v. United States*[3] the Supreme Court reversed a gambling conviction that was based on evidence obtained by means of a bug placed, without prior judicial authorization, upon the outside of a phone booth that the defendant had used. In both cases, the Court held electronic surveillance subject to the requirements of the fourth amendment.[4] The constitutional defect found in *Berger* was that the statute contained inadequate procedural standards and safeguards.[5] The *Katz* Court held that, although the bug would have been constitutional if prior judicial approval had been obtained, failure to obtain such approval was fatal.[6]

Title III of the Omnibus Crime Control and Safe Streets Act of 1968[7] was

1. 388 U.S. 41 (1967).

2. A "bug" is a device used to intercept oral communications not transmitted by wire. It is to be distinguished from a wiretap which is used to intercept communications transmitted by wire. Both are included in the terms "electronic eavesdropping" and "electronic surveillance." For a discussion of the various devices that may be used to conduct surveillance see A. Westin, Privacy and Freedom 67-89 (1967).

3. 389 U.S. 347 (1967).

4. Id. at 353; 388 U.S. at 50-53.

5. 388 U.S. at 58-60. The following is a list of the defects found in the New York statute taken from Committee Report, Judicial Procedures for National Security Electronic Surveillance, 29 Record of N.Y.C.B.A. 751, 753 (1974) (analyzing S. 2820, an amendment to Title III proposed by Senator Nelson) [hereinafter cited as Committee Report]: "1. It failed to provide that a warrant could be issued only upon a showing of probable cause. 2. It failed to require a description with particularity of the place to be searched and the person or thing to be seized. 3. It failed to require a description with particularity of the crime that had been, was being, or was about to be committed. 4. It failed to require a description with particularity of the type of conversation to be seized. 5. It failed to place any limitations on the officer executing the eavesdropping order which would prevent his searching unauthorized areas, and prevent his searching further once the property sought had been seized. 6. It failed to require a showing of probable cause in seeking a renewal of the eavesdropping order. 7. It failed to require dispatch in executing the order. 8. It failed to require that the officer to whom the order was issued return to the issuing court and show what had been seized. 9. It failed to require a showing of exigent circumstances to overcome the defect of not giving prior notice to those whose privacy had been invaded. 10. It failed to limit such orders to a time period equivalent to a single search, but instead authorized eavesdropping for a two-month period, which amounted to a series of searches and seizures pursuant to a single showing of probable cause."

6. 389 U.S. at 358-59.

7. 18 U.S.C. §§ 2510-20 (1970). The Act has been referred to by at least one of its critics as

enacted in an attempt to comply with *Katz* and *Berger*.[8] Section 2518 of that title contains the procedural requirements for obtaining an "order"[9] authorizing electronic surveillance,[10] and section 2511(3) specifies some of the types of surveillance to which the title does not extend.[11]

In *United States v. United States District Court (Keith)*[12] the Supreme Court held that the fourth amendment requires that judicial approval be obtained before the government conducts electronic surveillance of domestic organizations for the purpose of gathering national security intelligence. Since no warrant had been obtained in that case, it was unnecessary to consider the question of whether the procedural requirements of Title III are applicable to such surveillances, and the Court declined to do so.[13] More recently, in *Zweibon v. Mitchell*,[14] the Court of Appeals for the District of Columbia was divided over the issue. In *Zweibon*, the Court of Appeals sat en banc to consider the legality of a warrantless wiretap placed on the telephones of members of the Jewish Defense League for the purpose of gathering intelligence information concerning activities of that group which might have been harmful to America's relations with the Soviet Union. The majority of the court was of the opinion that the fourth amendment requires that a judicial warrant be obtained before a wiretap is installed on a "domestic organization that is neither the agent of nor acting in collaboration with a foreign power"—even where the activities of such a group endanger the national security by antagonizing a foreign power.[15]

Judge Wright, speaking for the plurality, stated that, "Congress intended the procedures and remedies of Title III to apply to all Executive surveillance which, under the Constitution, must be initiated pursuant to judicial warrant."[16] Judge Wilkey, with whom Judge MacKinnon was in substantial agreement and who concurred with the plurality on the constitutional issues, "strongly disagree[d] with the plurality's view that the strict procedural requirements of Title III—and, concomitantly, the damages provision con-

---

the "End to Privacy Act." S. Rep. No. 1097, 90th Cong., 2d Sess. 182 (1968) (Views of Senator Fong) [hereinafter cited as Senate Report].

8. Senate Report, supra note 7, at 66.

9. An "order" under the federal statute would be a "warrant" in most other contexts. For consistency "warrant" will be used herein except where the context requires otherwise.

10. 18 U.S.C. § 2518 (1970). In United States v. Turner, No. 73-2740 at 18-19 (9th Cir., July 24, 1975) (per curiam), the Ninth Circuit became the tenth of the circuits to uphold the constitutionality of Title III. The Tenth Circuit was the first, United States v. Cox, 449 F.2d 679 (10th Cir. 1971), cert. denied, 406 U.S. 934 (1972), and the First shall be last.

11. 18 U.S.C. § 2511(3) (1970). This includes the so-called "national security proviso." Zweibon v. Mitchell, 516 F.2d 594, 641 & n.219 (D.C. Cir. 1975) (plurality opinion); see text accompanying notes 19 & 34 infra.

12. 407 U.S. 297, 321 (1972). This decision is called the Keith case after District Judge Damon Keith against whom this mandamus proceeding was brought in order to prevent disclosure of electronic surveillance information to a criminal defendant.

13. Id. at 321-22; see Senate Report, supra note 7, at 94.

14. 516 F.2d 594 (D.C. Cir. 1975) (en banc).

15. Id. at 614 (plurality opinion); id. at 689 (Wilkey, J., concurring & dissenting).

16. Id. at 669 (plurality opinion).

tained in section 2520—are applicable to these special kinds of surveillance."[17] In response to *Zweibon*, Attorney General Levi said that, "[i]t is the position of the Department of Justice . . . that such surveillance is not regulated by the special procedural provisions of Title III."[18]

This Note will explore the arguments on both sides of the dispute regarding the applicability of Title III as well as the more important procedural requirements of section 2518. The analysis will encompass the underlying constitutional and policy considerations and the applicability of those considerations in the context of electronic surveillance that is intended to produce intelligence information rather than evidence of criminal activity.

II. The Dispute: The Applicability of Title III

A. *Background: The Title III Disclaimer*[19]

Section 2511(3) of Title 18 of the United States Code provides:

> Nothing contained in this chapter or in section 605 of the Communications Act of 1934 . . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.[20]

On its face, this provision would appear to anticipate that, once the courts resolved the questions related to the President's power to conduct electronic surveillance without a warrant—which questions were unresolved when the provision was written—the procedural requirements of the rest of Title III would apply in all cases in which, as a matter of constitutional law, the President must obtain a judicial warrant. The issue is not so easily resolved, however, since the procedural requirements of the rest of Title III were

---

17. Id. at 692-93 (Wilkey, J., concurring & dissenting); see id. at 706 (MacKinnon, J., concurring & dissenting).

18. Department of Justice Release (July 9, 1975). The Justice Department is apparently in the process of developing its own guidelines, but it has declined to make them public. N.Y. Times, Aug. 14, 1975, at 1, col. 6; see Address by the Hon. Edward H. Levi, A.B.A. Convention, Department of Justice Release 9-18 (August 13, 1975) [hereinafter cited as Levi Address].

19. "Disclaimer" is the term ordinarily used to characterize 18 U.S.C. § 2511(3) (1970). E.g., Zweibon v. Mitchell, 516 F.2d 594, 663 (D.C. Cir. 1975) (plurality opinion); id. at 693 (Wilkey, J., concurring & dissenting). The term "saving clause" has also been used. Levi Address, supra note 18, at 12.

20. 18 U.S.C. § 2511(3) (1970).

designed for use in the context of criminal investigations,[21] and some of those provisions may be inapplicable in an intelligence gathering context. For example, under section 2518(3)(a), the judge who issues a warrant authorizing the interception of wire or oral communications must first determine that "there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter . . . ."[22] Since section 2516 lists only criminal offenses,[23] this provision is obviously not designed for use by a judge authorizing a wiretap intended to afford government officials advance warning of non-criminal activities of domestic groups that may antagonize foreign powers.

B. *Background: The* Keith/Zweibon *Gap*

In *Keith*, the Supreme Court held that a warrant is required in cases involving the domestic aspects of national security intelligence gathering,[24] and in *Zweibon* the Court of Appeals extended that requirement to cases with a foreign affairs aspect.[25] These cases, and perhaps others, fall within a gap between ordinary criminal surveillance to which Title III plainly applies and that category of surveillance, which the courts have not yet defined,[26] for which no warrant need be obtained. The issue becomes, therefore, what standards and procedures must be complied with in order to obtain the requisite warrant in the *Keith/Zweibon* situation?

There are three possibilities: the courts could apply Title III, making such modifications as are found necessary to reconcile the intent of Congress with

---

21. See Zweibon v. Mitchell, 516 F.2d 594, 695-96 (D.C. Cir. 1975) (Wilkey, J., concurring & dissenting); Hearings on Practices and Procedures of the Department of Justice for Warrantless Wiretapping and Other Electronic Surveillance Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary, 92d Cong., 2d Sess. 8 (1972) (remarks of Senator Kennedy) [hereinafter cited as 1972 Hearings]; Levi Address, supra note 18, at 12; note 54 infra and accompanying text.

22. 18 U.S.C. § 2518(3)(a) (1970).

23. Id. § 2516(1)(a)-(g) (1970).

24. 407 U.S. at 314-21; accord, United States v. Smith, 321 F. Supp. 424, 429 (C.D. Calif. 1971).

25. 516 F.2d at 653-55.

26. Assuming that Zweibon is upheld, the only category left is national security surveillance of foreign powers, their agents and collaborators. The Zweibon plurality expressed, in dictum, the view that the warrant requirement applies even to that category of surveillance. Zweibon v. Mitchell, 516 F.2d 594, 651 (D.C. Cir. 1975) (plurality opinion); accord, Joint Hearings on Warrantless Wiretapping and Electronic Surveillance Before the Subcomm. on Administrative Practice and Procedure & the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary and the Subcomm. on Surveillance of the Senate Comm. on Foreign Relations, 93d Cong., 2d Sess. 72 (1974) (testimony of Ramsey Clark) [hereinafter cited as 1974 Hearings]; id. at 310 (testimony of William Ruckelshaus). Contra, United States v. Butenko, 494 F.2d 593, 606 (3d Cir.), cert. denied, 419 U.S. 881 (1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974); United States v. Hoffman, 334 F. Supp. 504, 507 (D.D.C. 1971). See generally Note, Foreign Security Surveillance and the Fourth Amendment, 87 Harv. L. Rev. 976 (1974) [hereinafter cited as Harv. Note].

the unique requirements of intelligence gathering;[27] the courts could disregard Title III and begin to develop constitutional requirements on an ad hoc basis as was done in *Berger* and *Katz* prior to the enactment of Title III;[28] or, finally, the Congress could enact legislation amending Title III. This last alternative was suggested in *Keith*,[29] and some movement has been made in that direction.[30]

C. *The* Zweibon *Plurality's Position*

The *Zweibon* plurality took the position that Title III applies to all electronic surveillance which must be initiated by a warrant. The plurality explained that section 2511 makes all electronic surveillance illegal except as provided elsewhere in Title III.[31] It interpreted the disclaimer in subsection three to be an expression of Congress' intent to make the application of Title III dependent upon future constitutional adjudication by the courts.[32] In other words, in the plurality's view, Congress intended Title III to apply to any electronic surveillance which the courts might hold to be constitutionally subject to a warrant requirement. Four factors weighed in favor of this conclusion. First, Title III represents an attempt by Congress to treat the field of electronic surveillance in a comprehensive manner.[33] The creation or recognition of exceptions to the requirements of that title would therefore be in derogation of congressional intent.[34] Second, one of the policies underlying

---

27. This was suggested by the Zweibon plurality, 516 F.2d at 669, and criticized by the minority. Id. at 697 (Wilkey, J., concurring & dissenting); id. at 707 (MacKinnon, J., concurring & dissenting).

28. See notes 5-6 supra and accompanying text. See also notes 36, 44 infra and accompanying text.

29. 407 U.S. at 322-33.

30. See Report on Warrantless Wiretapping and Electronic Surveillance by the Subcomm. on Surveillance of the Senate Comm. on Foreign Relations & the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary, 94th Cong., 1st Sess. 11 n.1 (Comm. Print 1975); 1974 Hearings, supra note 26, at 4 (opening statement of Senator Kennedy); id. at 7 (opening statement of Senator Muskie).

31. 516 F.2d at 659.

32. Id. at 665-66.

33. Id. at 667-68; see United States v. United States Dist. Ct., 407 U.S. 297, 302 (1972); Senate Report, supra note 7, at 69.

34. Congress was careful to specify the exceptions it sought to create. They include: the national security proviso, FCC personnel in the normal course of their duties and switchboard operators and telephone company personnel in the normal course of their duties. 18 U.S.C. §§ 2511(2), 2511(3) (1970). There is apparently only one judicially recognized exception. Simpson v Simpson, 490 F.2d 803, 809 (5th Cir.), cert. denied, 419 U.S. 897 (1974) (no civil cause of action for wiretapping by former husband—congressional intent was directed at organized crime). The exception is a limited one however. See Remington v. Remington, 393 F. Supp. 898, 901 (E.D. Pa 1975) (court could not, as a matter of law, hold gross invasions of individual privacy by unknown persons representing spouse to be not included in statutory proscription). On the danger of creating exceptions, see 1974 Hearings, supra note 26, at 234-35 (testimony of Nicholas Katzenbach); id. at 293 (testimony of Senator Nelson); 1972 Hearings, supra note 21, at 60-62 (statement of Nathan Lewin, former Assistant to Solicitor General).

the statute is uniformity.[35] Congress sought to establish one uniform set of standards and procedures that would apply to all electronic surveillance. This policy might easily be frustrated if the courts were to embark upon a program that would require the district courts to formulate their own standards and procedures on an ad hoc basis.[36] Third, the plurality recognized the need, on the part of the courts and the Executive, for clear guidance.[37] Finally, the plurality stated that the Title III standards and procedures are "salutary prophylactic measures designed to protect privacy interests while still accommodating the legitimate Executive need to conduct surveillance,"[38] and noted, later in its opinion, that these standards and procedures were probably the same as those which the courts would develop in any event.[39] This is particularly likely in view of the fact that the standards and procedures derive in large part from *Berger* and *Katz*.

D. *The Minority Position*

Judge Wilkey was unpersuaded by the plurality's reasoning. In his view the section 2511 disclaimer represented the intent of Congress to avoid legislating with respect to national security surveillance, whether or not subject to a constitutional warrant requirement.[40] He explained that in many instances the primary purpose of electronic surveillance is not the gathering of evidence of criminal activity, but rather, the gathering of information necessary to protect the national security.[41] Judge Wilkey pointed out that "the interrelated provisions of the Act are often totally inapposite to informational surveillances."[42]

Judge Wilkey focused on the last sentence of the disclaimer which makes "reasonableness" the test for admission into evidence of information gathered pursuant to the President's national security and foreign affairs powers.[43] He construed this provision to require the kind of ad hoc determinations of reasonableness which the plurality sought to avoid.[44] The legislative history of the provision is ambiguous:[45] it supports Judge Wilkey's view that reason-

---

35. 516 F.2d at 667; accord, Senate Report, supra note 7, at 66, 69.

36. The ad hoc approach has been criticized because: first, very few national security surveillances become the subject of litigation; second, since most judicial decisions will be made in camera there will be few precedents; and third, judges will perforce constantly be confronting national security surveillance as an original question. See Harv. Note, supra note 26, at 995-96.

37. 516 F.2d at 667-68.

38. Id. at 668.

39. Id. at 668-69 & n.263.

40. Id. at 693 (Wilkey, J., concurring & dissenting).

41. Id. (Wilkey, J., concurring & dissenting).

42. Id. at 696 (Wilkey, J., concurring & dissenting).

43. 18 U.S.C. § 2511(3) (1970); see 516 F.2d at 696-97 (Wilkey, J., concurring & dissenting), citing Senate Report, supra note 7, at 94.

44. 516 F.2d at 697 (Wilkey, J., concurring & dissenting); see note 36 supra and accompanying text. See generally Schwartz, The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order," 67 Mich. L. Rev. 455, 490-93 (1969) [hereinafter cited as Schwartz I].

45. Senate Report, supra note 7, at 94. Both the plurality and Judge Wilkey quoted extensively

ableness is the test of admission of all national security intelligence, but it also supports the position that reasonableness is the test of admission only where no warrant is constitutionally required.

Both Judge Wilkey and Judge MacKinnon emphasized what is probably the weakest link in the plurality's argument, *i.e.*, the probable cause standard set up in Title III. The plurality had suggested that section 2511(3) should be read to incorporate the appropriate standard of probable cause into section 2518 when intelligence gathering is involved.[46] Judge MacKinnon, on the other hand, pointed out that "Congress certainly did not intend the statute to be dissected in this manner."[47] Judge Wilkey remarked that, "[i]f Congress had intended to legislate with regard to information-gathering surveillances . . . it would not have left it to the courts to guess which sections to enforce."[48] These arguments are particularly convincing in light of the fact that the probable cause provisions lie "at the heart of Title III."[49]

E. *The Basic Disagreement*

At the core of the disagreement over the applicability of Title III to informational surveillance lies the difference between the problems involved in gathering national security intelligence by means of electronic surveillance and those involved in uncovering evidence of criminal activity by the same means. The plurality believed this difference to be sufficiently slight to require only a minor modification of the statute's probable cause requirement.[50] But Judges Wright and MacKinnon believed it to be so great as to require the courts to rewrite much of the statute.[51] The difference, whatever its magnitude, was recognized in *Keith*:

> [D]omestic security surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some

---

from this page. 516 F.2d at 665-66 n.240 (plurality opinion); id. at 693-94 (Wilkey, J., concurring & dissenting).

46. 516 F.2d at 669-70 (plurality opinion). The plurality's theory was that, since under 18 U.S.C. § 2511(3) (1970) nothing in Title III may disturb the President's constitutional power, and since the probable cause standard in section 2518 and the list of crimes in section 2516 would impair the President's power to conduct non-criminal surveillance, those sections should be read so as to include, implicitly, an appropriate standard of probable cause under section 2518 and national security intelligence gathering as a legitimate objective under section 2516.

47. 516 F.2d at 707 (MacKinnon, J., concurring & dissenting).

48. Id. at 698 (Wilkey, J., concurring & dissenting).

49. Id. at 697 (Wilkey, J., concurring & dissenting).

50. Id. at 669-70 (plurality opinion).

51. Id. at 696-97 (Wilkey, J., concurring & dissenting); id. at 706-07 (MacKinnon, J., concurring & dissenting).

possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.[52]

It should be pointed out, however, that Title III did not result from concern over "conventional types of crime." When conventional crimes such as assault, robbery, murder, rape or others are under investigation, electronic surveillance is of limited value because these crimes involve relatively little advance planning between co-conspirators.[53] Indeed, this kind of crime is frequently committed by individuals acting alone. Electronic surveillance is most useful in the investigation of organized crime and offenses such as gambling or narcotics, and it is organized crime to which Title III primarily addresses itself.[54]

The use of intelligence gathering surveillance is by no means unique to the national security field. In fact, the sort of surveillance techniques used in the investigation of organized crime frequently involve what is referred to as the gathering of " 'strategic' intelligence,"[55] *i.e.*, the surveillance of "known" criminals in order to obtain advance information regarding criminal enterprises in which they may be involved. The purpose of such surveillance is analogous to that of national security surveillance in that both are intended to produce intelligence information.[56]

It is likely that Congress was aware of the nature of "strategic intelligence" gathering and of its value in the investigation of organized crime when it enacted Title III.[57] Yet the probable cause requirement clearly outlaws the unfocused gathering of "strategic intelligence" in a criminal context.[58] One

52. United States v. United States Dist. Ct., 407 U.S. 297, 322 (1972).

53. Schwartz I, supra note 44, at 469, quoting Hearings on Controlling Crime Through More Effective Law Enforcement Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary, 90th Cong., 1st Sess. 957-58 (1967) (testimony of Prof. G. Robert Blakey).

54. United States v. Kahn, 415 U.S. 143, 151 (1974); Simpson v. Simpson, 490 F.2d 803, 806 (5th Cir.), cert. denied, 419 U.S. 897 (1974); Senate Report, supra note 7, at 70-74; Schwartz, Six Years of Tapping and Bugging, 1 Civ. Lib. Rev. 26 (Summer 1974) [hereinafter cited as Schwartz II].

55. Zweibon v. Mitchell, 516 F.2d 594, 648 (D.C. Cir. 1975) (plurality opinion); Schwartz I, supra note 44, at 468.

56. See Schwartz II, supra note 54, at 30-31; Schwartz I, supra note 44, at 469-70 & n.65. "Strategic intelligence" gathering is to be distinguished from the situation where law enforcement authorities have probable cause with respect to one or more individuals and employ electronic surveillance in order to learn who else is involved as well as the extent of the criminal enterprise. Such a situation occurs most often in cases involving minimization which is discussed in part III, section D, infra. See, e.g., United States v. Quintana, 508 F.2d 867, 874-75 (7th Cir. 1975); United States v. James, 494 F.2d 1007, 1019 (D.C. Cir. 1974); United States v. Cox, 462 F.2d 1293, 1300-01 (8th Cir. 1972), cert. denied, 417 U.S. 918 (1974).

57. See Schwartz II, supra note 54, at 31; Schwartz I, supra note 44, at 469-70 & n.65.

58. United States v. Bernstein, 509 F.2d 996, 999 (4th Cir. 1975), petition for cert. filed, 44 U.S.L.W. 3030 (U.S. July 22, 1975) (No. 74-1486); United States v. Tortorello, 480 F.2d 764, 779 (2d Cir.), cert. denied, 414 U.S. 866 (1973). The Department of Justice once took the position that under Keith domestic intelligence gathering is prohibited, and that Title III would have to be amended in order to permit it. 1972 Hearings, supra note 21, at 23-24 (testimony of Mr. Maroney). In 1969 Professor Schwartz presciently inquired, "if the Act does not grant law

might well argue that the policy underlying Title III prohibits intelligence gathering surveillance regardless of who it is directed against, unless it falls within the category of surveillance for which no warrant is necessary. Of course, under this interpretation of the statute mere intelligence gathering, even with a warrant, would be impermissible, and it seems unlikely that the courts will construe the statute so as to prohibit entirely a category of surveillance with respect to which Congress sought not to legislate.[59]

If intelligence gathering surveillance is not banned completely by Title III, and if the applicability of the Title III safeguards depends upon the magnitude of the difference between national security surveillance and ordinary criminal surveillance, then it becomes important to examine the Title III safeguards in order to determine whether the difference is great enough to make them inappropriate in the national security context.

III. The Title III Safeguards and National Security Intelligence Gathering

In addition to the probable cause requirement, section 2518 contains several safeguards which may be either inappropriate, not constitutionally required or in need of modification for national security intelligence gathering. The balance of this Note will be devoted to an examination of the most significant of those safeguards which include:

1) the particularization requirements:
   a) identity of the subject
   b) nature of the communication
2) the time provisions
3) the minimization requirement
4) the record keeping and warehousing provisions
5) the notice requirement

A. *Particularization: The Subject*

The particularization requirement derives from the fourth amendment.[60] In *Berger* this fourth amendment requirement was said to be of peculiar impor-

---

enforcement officers the power to obtain allegedly crucial strategic information, will we not again experience the same kind of widespread flouting of clear legal limitations that has recently come to light?" Schwartz I, supra note 44, at 471 (footnote omitted). In 1974 the Roscoe Pound-American Trial Lawyers Foundation adopted, by a substantial majority, the following recommendation: "There should be no electronic surveillance for domestic intelligence purposes." Annual Chief Justice Earl Warren Conference on Advocacy in the United States, June 7-8, 1974, Privacy In A Free Society, Final Report 11 (1974).

59. Even the Zweibon plurality conceded its legitimacy. 516 F.2d at 669-70 & n.268; see Senate Report, supra note 7, at 69; Schwartz I, supra note 44, at 490.

60. U.S. Const. amend. IV, provides, in part, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." If a warrant describes a particular conversation to be intercepted from a particular location, then the constitution is probably satisfied notwithstanding a failure to name the person to be overheard. See United States v. Fiorella, 468 F.2d 688, 691 (2d Cir. 1972), cert. denied, 417 U.S. 917 (1974). Title III goes beyond the constitutional requirement and provides that the speaker must be named if that person is "known." Id.

tance in the context of electronic surveillance.[61] Section 2518(1)(b)(iv) provides that an application for a warrant must include the name of the persons to be overheard, and section 2518(4)(a) requires that each authorizing order specify the identity of the person subject to the surveillance. As the Supreme Court noted in *Keith*, however, "[t]he exact targets of [security intelligence] surveillance may be more difficult to identify than in surveillance operations"[62] of a conventional nature. It can be argued, on the basis of that language, that the identification requirement should be relaxed or dispensed with when intelligence gathering is involved. In view of the construction which the Supreme Court has placed on the identification requirement, however, it is doubtful whether a relaxation of the requirement is necessary.

In *United States v. Kahn*[63] the Supreme Court considered a warrant authorizing the tapping of telephones used by Irving Kahn and "others as yet unknown."[64] Kahn and his wife were later indicted on gambling charges. The evidence against Mrs. Kahn included an intercepted conversation between herself and a "known gambling figure."[65] At a suppression hearing this conversation was ruled inadmissible as being outside the scope of the warrant on the ground that Mrs. Kahn was not a person "as yet unknown."[66] A divided Court of Appeals affirmed, but the Supreme Court reversed,[67] holding that the statute requires the naming of a person in the application or interception order only when the law enforcement authorities have probable cause to believe that the individual is "committing the offense" for which the wiretap is sought.[68]

---

61. 388 U.S. at 56, citing Osborn v. United States, 385 U.S. 323 (1966) (informer recorded his own planned conversation with suspect); Silverman v. United States, 365 U.S. 505 (1961) ("spike mike" used to monitor conversation in alleged gambling premises); On Lee v. United States, 343 U.S. 747 (1952) (informer wore transmitter during conversation with suspect); Goldman v. United States, 316 U.S. 129 (1942) (detectaphone used to record conversations between informer and suspect); see Schwartz I, supra note 44, at 464-65 & n.45. On the importance of the identification requirement, see United States v. Curreri, 368 F. Supp. 757, 760 (D. Md. 1973), aff'd sub nom. United States v. Bernstein, 509 F.2d 996, 999-1001 (4th Cir. 1975), petition for cert. filed, 44 U.S.L.W. 3030 (U.S. July 22, 1975) (No. 74-1486).

62. 407 U.S. at 322 (1972).

63. 415 U.S. 143 (1974).

64. Id. at 145.

65. Id. at 147.

66. Id. at 149.

67. Kahn v. United States, 471 F.2d 191 (7th Cir. 1972), aff'd & rev'd in part, 415 U.S. 143 (1974).

68. 415 U.S. at 155; accord, United States v. Doolittle, 507 F.2d 1368 (5th Cir.), aff'd en banc, 518 F.2d 500 (5th Cir. 1975), petition for cert. filed, 44 U.S.L.W. 3230 (U.S. Oct. 14, 1975) (No. 75-513); United States v. Martinez, 498 F.2d 464 (6th Cir. 1974), cert. denied, 419 U.S. 1056 (1975); see United States v. Donovan, 513 F.2d 337 (6th Cir. 1975), petition for cert. filed, 44 U.S.L.W. 3094 (U.S. Aug. 19, 1975) (75-212) (suspect should have been named); United States v. Bernstein, 509 F.2d 996 (4th Cir. 1975), petition for cert. filed, 44 U.S.L.W. 3030 (U.S. July 22, 1975) (No. 74-1486) (at time of first application probable cause existed with respect to suspect, but he was not "known" so failure to name him was not violative of the statute; at time of extension the suspect was "known" and failure to name him required suppression).

Thus, the identification requirement would seem to be a flexible one. So that in an intelligence gathering situation, when "[t]he exact targets . . . may be . . . difficult to identify,"[69] the failure to identify the target will not violate the statute. On the other hand, where the target is identifiable, there seems little reason why he or she should not be named.

The identification requirement is not just an important part of the fourth amendment, it is also a part of an integrated statute.[70] Under present law notice must be given to those named in the warrant,[71] but notice need be given to the unnamed subjects of surveillance only in the discretion of the court.[72] Justice Department officials have argued that the notice requirement should be abrogated in the national security field.[73] If their arguments are rejected by the courts, then they would naturally want the identification requirement limited in order to reduce the impact of the notice requirement.

If the only justification for limiting the identification requirement is to avoid giving notice, then it is likely that the argument for limitation would fail,[74] and in view of the flexibility of the identification requirement it is difficult to justify a limitation on any other ground. A warrant that fails to identify its subject would look a great deal like a general warrant, and considerably more authority than unsupported dictum from *Keith* should be required before it is permitted.

B. *Particularization: The Conversation*

Title III also requires particularity with respect to the conversations to be overheard.[75] Like the identification requirement, this requirement derives from the fourth amendment which provides that warrants specify the "things

---

69. 407 U.S. at 322.

70. See notes 74-75 infra.

71. 18 U.S.C. § 2518(8)(d) (1970).

72. Id.; see United States v. Curreri, 368 F. Supp. 757, 760 (D. Md. 1973), aff'd sub nom. United States v. Bernstein, 509 F.2d 996 (4th Cir. 1975), petition for cert. filed, 44 U.S.L.W. 3030 (U.S. July 22, 1975) (No. 74-1486); United States v. Ianelli, 339 F. Supp. 171, 173-74 (W.D. Pa. 1972, aff'd, 480 F.2d 907 (3d Cir. 1973), cert. denied, 417 U.S. 918 (1974).

73. See note 129 infra and accompanying text.

74. See United States v. Moore, 513 F.2d 485, 497-98 & n.34 (D.C. Cir. 1975), and United States v. Bernstein, 509 F.2d 996, 1000-01 (4th Cir. 1975), petition for cert. filed, 44 U.S.L.W. 3030 (U.S. July 22, 1975) (No. 74-1486), for discussions of the importance of, and relationship between, the notice and identification requirements. In Moore, the court explained that the government may not wait until there is absolutely no doubt as to probable cause before it must name a known individual. 513 F.2d at 496-97. Good faith is not an adequate justification for omission. Id. at 497. It has been held, however, that omission can be excused if those who should have been named were given notice and an opportunity to inspect the tapes and transcripts. United States v. Kilgore, 518 F.2d 496 (5th Cir. 1975).

75. 18 U.S.C. §§ 2518(1)(b)(iii), (4)(c) (1970). There exists a close relationship between the particularization and minimization requirements because what must be minimized is determined by reference to what has been specified. See Note, Minimization and the Fourth Amendment, 19 N.Y.L.F. 861, 870 (1974), in which the "plain view" doctrine, discussed in notes 79-81 infra and accompanying text, is considered in the context of minimization.

to be seized."[76] The requirement is thought to be an important one because it prevents the "seizure of one thing under a warrant describing another."[77] Language in *Keith* supports an argument that it is inapplicable to national security intelligence gathering surveillance.[78] Again, however, the judicial gloss on Title III may make a relaxation of this requirement unnecessary. The rule against "seizure of one thing under a warrant describing another" has been eroded in the conventional search and seizure situation by the "plain view" doctrine which permits seizure of items in the plain view of law enforcement authorities during the course of an otherwise lawful arrest[79] or search.[80] Section 2517(5) contains a statutory "plain view" provision which permits a retroactive judicial approval of the interception of conversations unrelated to those described in the warrant as long as the warrant was otherwise lawful.[81]

United States v. Denisio[82] is an extreme example of how "plain view" can operate. The warrant in that case authorized the interception of conversations related to robbery, bribery and conspiracy. The first few days of surveillance proved unproductive with respect to those offenses, but produced evidence of illegal bookmaking. On the basis of that evidence a search warrant was obtained, and a search of the defendant's residence produced, in addition to evidence of bookmaking, firearms for the possession of which the defendant was convicted. An attempt to suppress the wiretap evidence was unsuccessful. The result is entirely consistent with the "plain view" doctrine, but it is difficult to reconcile with the prohibition against seizure of one thing under a warrant describing another. It is difficult to quarrel with "plain view" because it usually comes up in situations where, as in *Denisio,* the individual involved has been engaged in a wide range of illegal activities. Nevertheless, the existence of the rule makes it difficult to justify the relaxation of the

---

76. U.S. Const. amend. IV; see notes 60-61 supra and accompanying text.

77. Marron v. United States, 275 U.S. 192, 196 (1927). The Marron case was relied upon in Berger. 388 U.S. at 58. See generally United States v. Tortorello, 480 F.2d 764, 778-81 (2d Cir.), cert. denied, 414 U.S. 866 (1973); United States v. Vega, 52 F.R.D. 503, 505-07 (E.D.N.Y. 1971).

78. 407 U.S. at 322-23.

79. Harris v. United States, 331 U.S. 145 (1947). The Marron case contributed to its own demise for, although it held that a search warrant could not be used to seize things other than those it described, it also held that when police officers made an arrest based on what they found pursuant to a legal search they could seize things in the arrestee's possession and control.

80. Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971).

81. 18 U.S.C. § 2517(5) (1970); see United States v. Moore, 513 F.2d 485, 502 & n.53 (D.C. Cir. 1975); United States v. Capra, 501 F.2d 267 (2d Cir. 1974), cert. denied, 420 U.S. 990 (1975) (court suppressed evidence where government failed to seek judicial approval promptly); United States v. Tortorello, 480 F.2d 764, 781-83 (2d Cir.), cert. denied, 414 U.S. 866 (1973); United States v. Mainello, 345 F. Supp. 863, 874-77 (E.D.N.Y. 1972); United States v. Sklaroff, 323 F. Supp. 296, 307 (S.D. Fla. 1971), aff'd, 506 F.2d 837 (5th Cir. 1975), cert. denied, 44 U.S.L.W. 3205 (U.S. Oct. 7, 1975) (No. 74-1249); United States v. Escandar, 319 F. Supp. 295, 300 (S.D. Fla. 1970); People v. Sher, 68 Misc. 2d 917, 923-24, 329 N.Y.S.2d 2, 9-10 (Greene County Ct. 1972) (Werker, J.).

82. 360 F. Supp. 715 (D. Md. 1973).

particularization requirement. Furthermore, the retention of the particularization requirement will help to assure that when individual privacy is to be invaded, law enforcement authorities will at least have something specific in mind when the warrant is sought.[83]

C. *The Time Provisions*

In *Berger*, the Supreme Court found that the time provisions of the New York statute were defective because they permitted what was, in effect, a series of intrusions pursuant to a single showing of probable cause.[84] The statute permitted interceptions up to 60 days in duration. Title III now limits electronic surveillance to 30 days,[85] and the courts of appeals have upheld this provision.[86] Although both statutes permit, or permitted, an unlimited number of extensions, and thus extremely long periods of surveillance, there is little objection to these provisions so long as a renewed showing of probable cause is required in order to obtain an extension. The important issue, with respect to time, is whether judicial review of continuing surveillance should occur often or seldom.[87]

Law enforcement officials assert that a 30 day limitation is excessively burdensome in the national security field, and suggest that 90 days would be more appropriate.[88] Legislation proposed by Senator Gaylord Nelson would

---

83. "Given the possibility of such long-term eavesdropping, Berger's requirement that the 'property' sought—the conversation—be described with particularity in the warrant becomes all the more important, at least theoretically. The wider the possible temporal or spatial area of a permissible search, the more important it is that the description of what is sought be precise, for imposing such a limitation may be the only way to discourage indiscriminate searches of extensive areas." Schwartz I, supra note 44, at 463. Compare United States v. Perillo, 333 F. Supp. 914, 921-22 (D. Del. 1971).

84. "[T]he Court in Berger reserved its strongest criticism of the New York law for the section allowing a dragnet-like surveillance for periods of sixty days and longer, saying it was, like the odious general warrants of colonial times, 'the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause.' " United States v. Cox, 462 F.2d 1293, 1303 (8th Cir. 1972), cert. denied, 417 U.S. 918 (1974) (footnotes omitted), quoting Berger v. New York, 388 U.S. 41, 59 (1967); see note 146 infra and accompanying text (a copy of a writ of assistance [general warrant] is provided in the appendix). A single showing of probable cause probably justifies more than one interception. See Schwartz I, supra note 44, at 463-64.

85. 18 U.S.C. § 2518(5) (1970).

86. See note 10 supra.

87. See United States v. Cox, 462 F.2d 1293, 1303-04 (8th Cir. 1972), cert. denied, 417 U.S. 918 (1974); United States v. Cafero, 473 F.2d 489, 497 (3d Cir. 1973), cert. denied, 417 U.S. 918 (1974); United States v Mainello, 345 F. Supp. 863, 872-73 (E.D.N.Y. 1972); Harv. Note, supra note 26, at 998.

88. "Unlike conventional criminal investigations [domestic intelligence inquiries] have no built-in necessary, automatic conclusion. They continue as long as there is a perceived threat." Levi Address, supra note 18, at 9; see 1974 Hearings, supra note 26, at 498-99 (testimony of William B. Saxbe) (Justice Department regulation provides for reauthorization every ninety days); 1972 Hearings, supra note 21, at 55 (testimony of Ramsey Clark) (three months is "often

limit surveillance to 15 days, but would permit extensions of national security surveillance without a de novo showing of probable cause.[89] It is doubtful whether either suggestion would be permitted under *Berger*, for both permit long-term interception on the basis of a single showing of probable cause.

Nevertheless, the Executive branch has a legitimate need to conduct effective national security intelligence gathering, and if the thirty day limit is too short to satisfy that need, then it should be changed. The *Keith* Court recognized that national security surveillance is often long-range in nature, and suggested that this might affect the standards to be applied in such cases.[90]

Whether the long-range nature of national security surveillance is unique is subject to question. Criminal investigations are often long-range enterprises,[91] and yet many judges require, pursuant to the discretion granted to them in Title III, progress reports as frequently as every five days.[92] This places a burden on the government and the courts, but it is a commendable practice: one indicative of the caution and concern for individual privacy that should be the hallmark of effective judicial supervision of electronic surveillance.[93] There is no evidence that this practice has decreased the effectiveness of surveillance directed at conventional crime, and there is no evidence that it will have such an effect in the national security context.

---

enough"). The ninety day regulation was still in effect when Zweibon was decided. 516 F.2d at 610 & n.26.

89. S. 2820, 93d Cong., 1st Sess. § 5(b)(5) (1973). A section analysis of the bill is found in 1974 Hearings, supra note 26, at 271-78. The bill is examined in Committee Report, supra note 5. Compare American Bar Association Project on Standards for Criminal Justice, Electronic Surveillance § 5.9 (1974) which suggests a fifteen day limit with a thirty day extension available only on showing of probable cause. It is difficult to understand why less should be required for renewal than for authorization. Logically, renewal should be more difficult. If the initial period has been fruitful, then it will be easy to make a stronger showing, but if it produced nothing, then some explanation should be required. See Harv. Note, supra note 26, at 998-99.

90. 407 U.S. at 322.

91. See Schwartz I, supra note 44, at 470. Between 1968 and 1973 the average federal criminal wiretap lasted for thirteen and a half days. On 3,492 installations during that period, 1,323 extensions were granted. This would indicate that many installations lasted for considerable periods of time. See Schwartz II, supra note 54, at 29. Between 1968 and 1970 the average national security tap lasted from 78.3 to 290.7 days. There was an average of about 100 such taps each year. Id. at 34.

92. See, e.g., United States v. Quintana, 508 F.2d 867, 875 (7th Cir. 1975); United States v. Cox, 462 F.2d 1293, 1301 (8th Cir. 1972), cert. denied, 417 U.S. 918 (1974).

93. The Act is constitutional because it requires strict judicial supervision. United States v. Martinez, 498 F.2d 464, 468 (6th Cir. 1974), cert. denied, 419 U.S. 1056 (1975). Section 801(d) of the original Act, which contained legislative fact finding, acknowledged the important role played by the judiciary in the protection of individual privacy. In the six years since Title III became effective only five or six requests for warrants have been denied by the judiciary. Schwartz II, supra note 54, at 33. A good example of close judicial supervision may be found in United States v. Bynum, 360 F. Supp. 400, 407-19 (S.D.N.Y.), aff'd, 485 F.2d 490 (2d Cir. 1973), vacated on other grounds, 417 U.S. 903 (1974) (frequently referring to District Judge Travia's continuing review of the wiretap involved).

Frequent judicial supervision provides a bulwark against unjustified intrusions into the sensitive areas of privacy and first amendment rights.[94] The innocent targets of national security surveillance are no less deserving of the protection afforded by time limitations than are innocent targets of conventional surveillance. Indeed, they may be more deserving of protection because they will be subjected to intrusions when there is no probable cause to believe they are committing a crime.

D. *Minimization*

Few of section 2518's provisions have been litigated more frequently than the minimization provision of subsection 5.[95] In a national security intelligence gathering context, good arguments can be made that minimization will be difficult if not impossible. Since there may be uncertainty regarding the targets of the surveillance, it may be difficult to decide to whom to listen.[96] Uncertainty regarding the nature of the conversations to be overheard may make it difficult to separate the relevant from the irrelevant.[97] Codes or foreign languages may be employed to confuse or mislead those conducting the surveillance.[98] Finally, the targets of surveillance may attempt to deceive law enforcement authorities by beginning their conversations in an innocent manner in the hope that after a few minutes the tap will be turned off.[99]

---

94. Former Assistant to the Solicitor General Nathan Lewin considers the time provisions to be a "substantial restraint," and to be among the "more effective practical checks" on abuses. 1972 Hearings, supra note 21, at 61.

95. See, e.g., United States v. Turner, No. 73-2740 (9th Cir., July 24, 1975) (per curiam); United States v. Armocida, 515 F.2d 29, 42-46 (3d Cir. 1975); United States v. Quintana, 508 F.2d 867 (7th Cir. 1975); United States v. Cafero, 473 F.2d 489 (3d Cir. 1973), cert. denied, 417 U.S. 918 (1974); United States v. King, 335 F. Supp. 523, 540-45 (S.D. Cal. 1971), rev'd on other grounds, 478 F.2d 494 (9th Cir.), cert. denied, 414 U.S. 826 (1973). See generally Note, Minimization and the Fourth Amendment, 19 N.Y.L.F. 861 (1974).

96. United States v. Turner, No. 73-2740 at 12, 15-17 (9th Cir., July 24, 1975) (per curiam); United States v. Capra, 501 F.2d 267, 274 (2d Cir. 1974), cert. denied, 420 U.S. 990 (1975); United States v. James, 494 F.2d 1007, 1019-20 (D.C. Cir. 1974); United States v. Cox, 462 F.2d 1293, 1301 (8th Cir. 1972), cert. denied, 417 U.S. 918 (1974); United States v. Falcone, 364 F. Supp. 877, 882 (D.N.J. 1973), aff'd, 505 F.2d 478 (3d Cir. 1974), cert. denied, 420 U.S. 955 (1975).

97. United States v. Turner, No. 73-2740, at 12 (9th Cir., July 24, 1975) (per curiam); United States v. Cirillo, 499 F.2d 872, 880 & n.6 (2d Cir.), cert. denied, 419 U.S. 1056 (1974); United States v. James, 494 F.2d 1007, 1020 (D.C. Cir. 1974), cert. denied, 419 U.S. 1020 (1975); United States v. Bynum, 485 F.2d 490, 500 (2d Cir. 1973), vacated on other grounds, 417 U.S. 903 (1974); United States v. Cox, 462 F.2d 1293, 1301 (8th Cir. 1972), cert. denied, 417 U.S. 918 (1974); United States v. LaGorga, 336 F. Supp. 190, 196 (W.D. Pa. 1971).

98. United States v. Turner, No. 73-2740 at 17 (9th Cir., July 24, 1975) (per curiam); United States v. Capra, 501 F.2d 267, 273 (2d Cir. 1974), cert. denied, 420 U.S. 990 (1975); United States v. Cirillo, 499 F.2d 872, 881 (2d Cir.), cert. denied, 419 U.S. 1056 (1974); United States v. James, 494 F.2d 1007, 1019 (D.C. Cir. 1974); United States v. Bynum, 360 F. Supp. 400, 412-13 (S.D.N.Y.), aff'd, 485 F.2d 490 (2d Cir. 1973), vacated on other grounds, 417 U.S. 903 (1974); United States v. Focarile, 340 F. Supp. 1033, 1048 (D. Md.), aff'd sub nom. United States v. Giordano, 469 F.2d 522 (4th Cir. 1972), aff'd on other grounds, 416 U.S. 505 (1974).

These considerations are by no means unique to the national security field. They have been successfully advanced and accepted in cases involving ordinary criminal surveillance. In *United States v. Quintana*,[100] the government intercepted all incoming and outgoing calls from the defendant's store and home for a period of 35 days. "Some 2000 calls were intercepted, while only 153 were ultimately found germane enough to be worth transcribing, and only 47 were used at trial."[101] The Court of Appeals for the Seventh Circuit held that surveillance of this kind was not a per se violation of the statute.[102] The Court explained that whether the minimization requirement has been complied with depends on a "case-by-case analysis of the reasonableness of [each] particular interception."[103] The Court held that the government had made a prima facie showing of reasonableness based upon the following factors: the criminal enterprise under investigation was a large and sophisticated narcotics conspiracy, and the surveillance was designed as much to learn the identity of co-conspirators and the extent of the conspiracy as it was to incriminate the defendant whose phone was tapped;[104] many conversations contained a mix of relevant and irrelevant conversations and there was no pattern of innocent conversation that would indicate to the agents monitoring the tap that the conversation should not be intercepted;[105] the authorizing judge exercised continuing supervision of the tap and required the government to submit reports at five-day intervals.[106]

Thus, although it is clear that national security surveillance can pose difficult minimization problems for law enforcement authorities, it is not at all clear that these difficulties will be any greater than in many criminal cases—unless it be assumed that members of organized crime or narcotics conspiracies are somehow less proficient at eluding law enforcement authorities than their counterparts in the fields of espionage and subversion. In addition, it is far from clear that, under present law, the minimization requirement is sufficiently inflexible to impose any substantial burden on law

---

Cir. 1974), cert. denied, 420 U.S. 955 (1975); United States v. Bynum, 360 F. Supp. 400, 412-13 (S.D.N.Y.), aff'd, 485 F.2d 490 (2d Cir. 1973), vacated on other grounds, 417 U.S. 903 (1974); cf. United States v. Cirillo, 499 F.2d 872, 880 n.6 (2d Cir.), cert. denied, 419 U.S. 1056 (1974).

100. 508 F.2d 867 (7th Cir. 1975). The Third Circuit appears to be in complete accord with Quintana. See United States v. Armocida, 515 F.2d 29, 42-46 (3d Cir. 1975).

101. 508 F.2d at 873.

102. Id.

103. Id. at 873-74.

104. Id. at 874; see United States v. Falcone, 364 F. Supp. 877, 885 (D.N.J. 1973), aff'd, 505 F.2d 478 (3d Cir. 1974), cert. denied, 420 U.S. 955 (1975); United States v. Focarile, 340 F. Supp. 1033, 1047 (D. Md.), aff'd sub nom. United States v. Giordano, 469 F.2d 522 (4th Cir. 1972), aff'd on other grounds, 416 U.S. 505 (1974); United States v. Escandar, 319 F. Supp. 295, 303 (S.D. Fla. 1970).

105. 508 F.2d at 875.

106. Id.; accord, United States v. Bynum, 485 F.2d 490, 501 (2d Cir. 1973), vacated on other grounds, 417 U.S. 903 (1974) (summaries and logs submitted at intervals of four to eight days); United States v. Escandar, 319 F. Supp. 295, 303 (S.D. Fla. 1970); see note 92 supra and accompanying text.

enforcement.[107] Indeed, the contrary appears to be the fact because under *Quintana* and similar cases all that is required is a good faith attempt to minimize[108]—a requirement that can hardly be expected to place an undue burden on any kind of surveillance.

E. *Warehousing and Record Keeping*

Under section 2518(8)(a), the fruits of electronic surveillance must, if possible, be recorded on tape in such a way as to prevent editing or alteration. Immediately after the warrant expires, the tapes must be presented to the issuing judge for sealing, and they must be preserved for ten years.[109] These provisions serve two functions: they preserve the integrity and accuracy of the recordings,[110] and they insure that a record will be available if the legality of the interception is later challenged.[111]

In *Zweibon* the original recordings were destroyed, and only summaries were available to the court.[112] Although the Justice Department has made conflicting representations regarding government policy with respect to record keeping,[113] it is clear that it would prefer to produce its own summaries of

---

107. The statute merely "requires that measures be adopted to reduce the extent of such interception to a practical minimum while allowing the legitimate aims of the Government to be pursued." United States v. Turner, No. 73-2740 at 15 (9th Cir., July 24, 1975) (per curiam).

108. United States v. Armocida, 515 F.2d 29, 44 (3d Cir. 1975); United States v. Quintana, 508 F.2d 867, 875 (7th Cir. 1975) (citing cases which stand for the proposition that frequent judicial review of surveillance makes it easier to find that a good faith attempt has been made); see United States v. Tortorello, 480 F.2d 764, 784 (2d Cir.), cert. denied, 414 U.S. 866 (1973) ("on the whole the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion."); United States v. Falcone, 364 F. Supp. 877, 886-87 (D.N.J. 1973), aff'd, 505 F.2d 478 (3d Cir. 1974), cert. denied, 420 U.S. 955 (1975); United States v. Scott, 331 F. Supp. 233, 248 (D.D.C. 1971), vacated & remanded, 504 F.2d 194 (D.C. Cir. 1974) (subsequent order on remand, not reported officially, was reversed at 516 F.2d 751 (D.C. Cir. 1975) [District Court suppressed all conversations intercepted in view of what it considered the agent's failure to observe minimization requirements—Court of Appeals found the minimization standard to be one of reasonableness which was comported with in all interceptions]).

109. 18 U.S.C. § 2518(8)(a) (1970).

110. United States v. Sklaroff, 506 F.2d 837 (5th Cir. 1975), cert. denied, 44 U.S.L.W. 3205 (U.S. Oct. 7, 1975) (No. 74-1249); Senate Report, supra note 7, at 104. The sealing and warehousing provisions also serve to preserve the confidential nature of the recordings. United States v. Falcone, 505 F.2d 478 (3d Cir. 1974), cert. denied, 420 U.S. 955 (1975); Senate Report, supra note 7, at 104. Nathan Lewin ranks the record keeping and warehousing provisions among the more effective practical checks on abuses. 1972 Hearings, supra note 21, at 61. A moderate delay in sealing can be excused if the government was acting in good faith. United States v. Poeta, 455 F.2d 117, 122 (2d Cir.), cert. denied, 406 U.S. 948 (1972).

111. United States v. Huss, 482 F.2d 38, 47-48 (2d Cir. 1973); Senate Report, supra note 7, at 104; see United States v. Bryant, 439 F.2d 642, 650-53 (D.C. Cir. 1971) (criminal conviction remanded because government had lost tapes sought by defendants).

112. 516 F.2d at 605 n.10 (plurality opinion).

113. Id.; cf. 1974 Hearings, supra note 26, at 449 (statement of John Shattuck and Leon Friedman of American Civil Liberties Union).

conversations for court inspection rather than original tapes. Apparently, the only justification advanced in favor of destruction is a concern for warehousing space.[114]

Despite its primary purpose, national security intelligence is often sought to be introduced in evidence in criminal trials. The *Zweibon* case is a classic example.[115] In the context of a criminal trial it becomes vitally important that accurate and complete records be made available. For example, if the government failed to minimize its interceptions, that fact would be unlikely to appear in summaries because summaries would not be made of irrelevant conversations. Another example of the importance of having original recordings rather than summaries may be found in *United States v. Huss*.[116] That case arose from a contempt proceeding that developed out of the same Jewish Defense League wiretaps involved in *Zweibon*.[117] At trial, a witness refused to answer questions posed by government attorneys on the ground that the questions were based on information gathered pursuant to an illegal wiretap. The issue became whether the questions were based on wiretap information or on an independent source untainted by the wiretap.[118] The trial judge concluded that there had been an independent, untainted source.[119] However, the witness claimed that actual tape recordings, which the government had destroyed, would prove the contrary, and that the destruction made it impossible for him to rebut the government's case.[120] His own case was particularly strong because he had his own tapes of conversations with one of the government's agents that indicated that he had been "fingered" by wiretaps.[121] The contempt order was vacated because the government had placed the witness in the absurd position of having to prove taint without all of the means necessary to do so.[122] A Second Circuit case decided after *Huss*[123] indicates that, where a strong showing of independent source is made, the destruction of tapes will not result in the suppression of evidence allegedly obtained through illegal wiretaps.[124]

Even if intelligence surveillance were not used in criminal trials, the warehousing provisions would still be important. There are both statutory and common law causes of action for illegal electronic surveillance.[125] In order to

114. See United States v. Huss, 482 F.2d 38, 48 (2d Cir. 1973).

115. Others are United States v. Butenko, 494 F.2d 593 (3d Cir.), cert. denied, 419 U.S. 881 (1974); United States v. Brown, 484 F.2d 418 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974).

116. 482 F.2d 38 (2d Cir. 1973). See also United States v. Bryant, 439 F.2d 642, 650-53 (D.C. Cir. 1971).

117. 516 F.2d at 668 n.256.

118. United States v. Huss, 482 F.2d 38, 42 (2d Cir. 1973).

119. Id. at 45.

120. Id. at 46-47. Under Alderman v. United States, 394 U.S. 165, 18 (1969), the government has the burden of persuasion to show lack of taint, but the defendant h rs a burden of going forward with evidence of taint.

121. United States v. Huss, 482 F.2d 38, 49 (2d Cir. 1973).

122. Id. at 51.

123. United States v. Garcilaso de la Vega, 489 F.2d 761 (2d Cir. 1974).

124. Id. at 764-65.

125. The statutory provision is contained in 18 U.S.C. § 252 (1970). Unde eibon this

prevail in such an action, the plaintiff must show that the surveillance violated either the fourth amendment or Title III. To require such a plaintiff to carry his burden of proof without accurate records of the surveillance would be just as absurd as requiring the witness in *Huss* to show taint under the same conditions.

F. *Notice*

One of the constitutional flaws the *Berger* Court found in the New York statute was its failure to afford notice to the targets of surveillance.[126] Section 2518(8)(d) represents an attempt to comply with *Berger*.[127] Subjects of surveillance must be given notice within a reasonable time from the termination of the period of the warrant. Absent judicial approval, notice may not be postponed beyond 90 days.[128] Former Attorneys General Richardson and Saxbe and former Deputy Attorney General Ruckelshaus have all asserted that this requirement is "obviously inappropriate for national security intelligence gathering surveillances."[129] The rationale behind this assertion appears to be that notice will "blow the cover" of the government, and impair or destroy the usefulness of the wiretap.[130] It is important to define the kind of notice involved. The notice required by *Berger* and the statute is post-search notice, not prior notice. Prior notice is neither constitutionally nor statutorily required.[131] Post-search notice is required after the surveillance terminates so that the subject of the surveillance will be able to vindicate his rights if the surveillance was illegal.[132]

In a large-scale, long-range intelligence operation, law enforcement authorities may be conducting a series of surveillances and may be relying on a broad range of sources of information.[133] Such an operation could be severely jeopardized by premature notification of even one target of surveillance, for

---

provision of Title III applies to national security surveillance. A common law cause of action was recognized in Bivens v. Six Unknown Named Agents of the Fed. Bureau of Narcotics, 403 U.S. 388 (1971).

126. 388 U.S. at 60.

127. See Senate Report, supra note 7, at 105.

128. 18 U.S.C. § 2518(8)(d) (1970). The Nelson bill, discussed at note 89 supra and accompanying text, contains a stricter provision that is examined in depth in Committee Report, supra note 5, at 764-66.

129. 1974 Hearings, supra note 26, at 17 (testimony of Elliot Richardson); see id. at 331 (testimony of William Ruckelshaus) (discussing surveillance of foreigners); id. at 493-94 (testimony of William Saxbe). But see 1972 Hearings, supra note 21, at 51-52 (testimony of Ramsey Clark).

130. 1974 Hearings, supra note 26, at 494 (testimony of William Saxbe).

131. See United States v. Martinez, 498 F.2d 464, 468 (6th Cir. 1974), cert. denied, 419 U.S. 1056 (1975).

132. United States v. Bernstein, 509 F.2d 996, 1000-01 (4th Cir. 1975), petition for cert. filed, 44 U.S.L.W. 3030 (U.S. July 22, 1975) (No. 74-1486); Committee Report, supra note 5, at 764; Senate Report, supra note 7, at 105; Schwartz II, supra note 54, at 33; Schwartz I, supra note 44, at 484; Harv. Note, supra note 26, at 999-1000; 1972 Hearings, supra note 21, at 61-62 (statement of Nathan Lewin) (notice is one of the more effective practical checks on abuses).

133. United States v. United States Dist. Ct., 407 U.S. 297, 322 (1972).

that person is likely to inform all of the others involved.[134] Similarly, a fruitful source of intelligence may be used for a period of time, and then terminated, in the hope that when future intelligence is needed the source will again be available. Such a source would be rendered useless if notice were given after the first surveillance because the target would always be suspicious thereafter.

The Act itself, of course, permits notice to be postponed upon an ex parte showing of good cause,[135] and the Senate Committee Report points out that in a national security context, notice could be postponed almost indefinitely[136]—an indication that the notice requirement was expected to be applied to such surveillance. Even if postponement were not available, however, the flexibility of the notice provision supports an argument that it be applied to intelligence gathering surveillances.

The courts have explained that the notice requirement "is not meaningless. It eliminates, insofar as practicable, the possibility of completely secret electronic eavesdropping and grants to the person involved an opportunity to seek redress . . . ."[137] and that it is "an absolutely necessary link in the chain of protective measures built into the statute."[138] In practice the provision has not been strictly enforced, however, and seldom does a failure to serve notice within 90 days or within the period permitted by any extension result in suppression.[139] The cases refer to the notice requirement as a "ministerial"[140] provision, and absent a deliberate attempt to flout the statute[141] there may be no remedy for a failure to give notice. If the defendant has actual knowledge,[142] or if he was not prejudiced by the delay,[143] suppression may be

---

134. See United States v. John, 508 F.2d 1134, 1139 (8th Cir.), cert. denied, 421 U.S. 962 (1975).

135. 18 U.S.C. § 2518(8)(d); see United States v. John, 508 F.2d 1134 (8th Cir.), cert. denied, 421 U.S. 962 (1975); United States v. Wolk, 466 F.2d 1143 (8th Cir. 1972).

136. Senate Report, supra note 7, at 105.

137. United States v. Eastman, 326 F. Supp. 1038, 1039 (M.D. Pa. 1971), aff'd, 465 F.2d 1057 (3d Cir. 1972).

138. Id.

139. E.g., id.; United States v. Chun, 386 F. Supp. 91 (D. Hawaii 1974).

140. United States v. Smith, 463 F.2d 710 (10th Cir. 1972); United States v. Lawson, 334 F. Supp. 612 (E.D. Pa. 1971). But see United States v. Eastman, 465 F.2d 1057, 1062 (3d Cir. 1972).

141. United States v. Eastman, 465 F.2d 1057, 1062 (3d Cir. 1972). But see United States v. Donovan, 513 F.2d 337, 343 (6th Cir. 1975), petition for cert. filed, 44 U.S.L.W. 3094 (U.S. Aug. 19, 1975) (75-212).

142. United States v. Wolk, 466 F.2d 1143, 1146 (8th Cir. 1972). But see United States v. Bernstein, 509 F.2d 996, 1004 (4th Cir. 1975), petition for cert. filed, 44 U.S.L.W. 3030 (U.S. July 22, 1975) (No. 74-1486).

143. United States v. Rizzo, 492 F.2d 443, 447 (2d Cir.), cert. denied, 417 U.S. 944 (1974); United States v. Smith, 463 F.2d 710 (10th Cir. 1972); United States v. LaGorga, 336 F. Supp. 190, 194 (W.D. Pa. 1971); United States v. Lawson, 334 F. Supp. 612, 616-17 (E.D. Pa. 1971); United States v. Cantor, 328 F. Supp. 561 (E.D. Pa. 1971), aff'd, 470 F.2d 890 (3d Cir. 1972). But see United States v. Bernstein, 509 F.2d 996, 1004 (4th Cir. 1975), petition for cert. filed, 44 U.S.L.W. 3030 (U.S. July 22, 1975) (No. 74-1486). In the Chun case, the court examined the

denied. Whether a failure to give notice gives rise to a civil cause of action is unknown—probably because those who have the right to bring such actions are unaware of the fact.

Perhaps the most insidious feature of electronic surveillance is its secrecy. The target's unawareness of the surveillance is at once the feature that makes it valuable and the feature that makes it susceptible of great abuse. Although it is important that the value of such surveillance be preserved for as long as necessary, it is equally important that the target be notified when secrecy is no longer necessary. Section 2518(8)(d) with its notification and postponement provisions is nothing more than a device by means of which both interests can be accommodated.[144]

IV. Conclusion

An analysis of the problems that law enforcement authorities are likely to face in the context of national security intelligence gathering reveals that these problems are usually not any greater than those faced in difficult criminal investigations. This analysis suggests that, at least until Congress can develop something better, it is desirable that the Justice Department proceed under, and that the courts apply, Title III to all surveillances to which the warrant requirement applies. Even Justice Department officials have conceded that, in the criminal context, "Title III works well,"[145] and there is little reason to believe that its provisions will be any less workable in the national security context. Perhaps the best argument in favor of applying Title III to national security intelligence gathering would be a warrant that failed to comply with the provisions discussed above. It would not contain the names of those whose conversations are expected to yield information. It would not describe the types of conversations anticipated. It would last as long as there was a perceived threat. The officials executing the warrant would not be required to minimize the intrusion. After the interception few records would remain, and recordings would be destroyed instead of being sealed by the issuing judge. Finally, the only targets of surveillance who would be notified would be those who were subsequently prosecuted—and then only in response to defense discovery motions.

It is instructive to recall that the writ of assistance against which James Otis unsuccessfully argued in 1761[146] contained similar features and became a

---

notice requirement closely and concluded that prejudice is a constitutional test, i.e., if there has been prejudice, then the Constitution has been violated notwithstanding compliance with the statute. United States v. Chun, 386 F. Supp. 91, 94 (D. Hawaii 1974).

144. The Nelson bill has been criticized because its postponement provision is not sufficiently flexible. Committee Report, supra note 5, at 765.

145. 1974 Hearings, supra note 26, at 494 (testimony of William Saxbe).

146. There exists no formal record of James Otis' Speech Against the Writs of Assistance. John Adams took notes of the speech however and G. R. Minot later expanded these notes into the version of argument which Adams revised. H. Commager, Documents of American History 45 (3d ed. 1947). Otis argued that the writ, which is reprinted in the appendix to this Note, contained the following illegal features (parenthetical indications after each refer to the numbers corresponding to the numbers of the constitutional shortcomings of the New York statute

major tool for oppression. The fourth amendment was fashioned to prohibit the use of such general writs, and Title III does not purport to be anything more than an attempt to conform with the requirements of the fourth amendment. Until it can be shown that Title III is in fact too burdensome and too inflexible to be applied in the context of national security intelligence gathering, its provisions should prevail.

Thomas I. Sheridan III

APPENDIX

Writ of Assistance

The following is a copy of the Writ of Assistance that was issued to "Surveyor & Searcher" Charles Paxton at the request of Thomas Lechmere, the "Surveyor General" of the Port of Boston, on December 2, 1761. The copy is taken from W. MacDonald, Documentary Source Book of American History 1606-1898, at 106-09 (1908). Although the writ does not indicate the fact, MacDonald, in his prefatory notes, informs us that the writ was effective until the demise of the Crown and for six months thereafter. Id. at 106. It was legalized by the Townshend Revenue Act of 1767 which is reprinted in id. at 143-46. This general warrant is included here for two reasons: first, the fourth amendment was largely an attempt to outlaw the Writ of Assistance and it is therefore important to understand what that document said; second, despite its importance, it is a difficult document to find. The reader should note that, in the manuscript MacDonald used, the words in brackets are interlined, and those in italics erased.

Prov. of Mass. Bay } George the third by the grace of God of Great Britan France & Ireland King Defender of the faith &c.

SEAL

To All & singular our Justices of the peace Sheriffs Constables and to all other our Officers and Subjects within our said Province and to each of you Greeting.

Know Ye that whereas in and by an Act of Parliament made in the *thir*[four]teenth year of [the reign of] the late King Charles the second *it is declared to be* [the Officers of our Customs & their Deputies are authorized and impowered to go & enter aboard any Ship or Vessel outward or inward bound for the purposes in the said Act mentioned and it is *also* in & by the said Act further enacted & declared that it shall be] lawful [to or] for any person or persons authorized by Writ of assistants under the seal of our Court of Exchequer to take a Constable Headborough or other publick

involved in Berger listed in note 5 supra): 1) it was directed to everyone; anyone could exercise the power it conferred; 2) it was perpetual (10); 3) probable cause was not required (1); 4) it was a general warrant, i.e., it authorized a search of any place for any things (2 & 4); 5) no oath was required; 6) there was no return (8).

Officer inhabiting near unto the place and in the day time to enter & go into any House Shop Cellar Warehouse or Room or other place and in case of resistance to break open doors chests trunks & other package there to seize and from thence to bring any kind of goods or merchandize whatsoever prohibited & uncustomed and to put and secure the same in *his Majestys* [our] Storehouse in the port next to the place where such seizure shall be made.

And Whereas in & by an Act of Parliament made in the seventh & eighth year of [the reign of the late] King William the third there is granted to the Officers for collecting and managing our revenue and inspecting the plantation trade in any of our plantations [the same powers & authority for visiting & searching of Ships & also] to enter houses or warehouses to search for and seize any prohibited or uncustomed goods as are provided for the Officers of our Customs in England by the said last mentioned Act made in the fourteenth year of [the reign of] King Charles the Second, and the like assistance is required to be given to the said Officers in the execution of their office as by the said last mentioned Act is provided for the Officers in England.

And Whereas in and by an Act of our said Province of Massachusetts bay made in the eleventh year of [the reign of] the late King William the third it is enacted & declared that our Superior Court of Judicature Court of Assize and General Goal delivery for our said Province shall have cognizance of all matters and things within our said Province as fully & amply to all intents & purposes as our Courts of King's Bench Common Pleas & Exchequer within our Kingdom of England have or ought to have.

And Whereas our Commissioners for managing and causing to be levied & collected our customs subsidies and other duties have [by Commission or Deputation under their hands & seal dated at London the 22d day of May in the first year of our Reign] deputed and impowered Charles Paxton Esquire to be Surveyor & Searcher of all the rates and duties arising and growing due to us at Boston in our Province aforesaid and [in & by said Commission or Deputation] have given him power to enter into [any Ship Bottom Boat or other Vessel & also into] any Shop House Warehouse Hostery or other place whatsoever to make diligent search into any trunk chest pack case truss or any other parcell or package whatsoever for any goods wares or merchandize prohibited to be imported or exported or whereof the Customs or other Duties have not been duly paid and the same to seize to our use In all things proceeding as the Law directs.

Therefore we strictly Injoin & Command you & every one of you that, all excuses apart, you & every one of you permit the said Charles Paxton according to the true intent & form of the said commission or deputation and the laws & statutes in that behalf made & provided, [as well by night as by day from time to time to enter & go on board any Ship Boat or other Vessel riding lying or being within or coming to the said port of Boston or any Places or Creeks thereunto appertaining such Ship Boat or Vessel then & there found to search & oversee and the persons therein being strictly to examine touching the premises aforesaid & also *according to the form effect and true intent of the said commission or deputation*] in the day time to enter & go into the vaults cellars warehouses shops & other places where any prohibited goods wares or merchandizes or any goods wares or merchandizes for which the customs or other duties shall not have been duly & truly satisfied and paid lye concealed or are suspected to be concealed, according to the true intent of the law to inspect & oversee & search for the said goods wares & merchandize, And further to do and execute all things which of right and according to the laws & statutes in this behalf shall be to be done. And we further strictly Injoin & Command you and every one of you that to the said Charles Paxton Esqr you & every one of you from time to time be aiding assisting

& helping in the execution of the premises as is meet. And this you or any of [you] in no wise omit at your perils. Witness Thomas Hutchinson Esq at Boston the day of December in the Second year of our Reign Annoque Dom 1761

By order of Court
N. H. Cler.

Removing Political Influence from Federal Law Enforcement Agencies

by William B. Spann, Jr.

PERIODICALLY throughout American history, corruption and scandal have rocked our federal government. Fortunately, the scandals rarely have involved the federal law enforcement agencies, for when the very bodies established to ferret out and prosecute wrongdoing are themselves involved in wrongdoing, the effect is indeed severe. The Teapot Dome scandal of 1924, the Department of Justice scandal in 1953, and the Watergate affair, among others, clearly evidence the dangers to a society governed by law when the enforcers of the law behave in lawless fashion.

The American Bar Association Special Committee to Study Federal Law Enforcement Agencies, of which I am chairman, has been at work for the past two years examining the problems illuminated by these events. The other members of the committee are Judge Christopher T. Bayley of the King County Superior Court, Seattle, Washington; Chester Bedell of Jacksonville, Florida; Justice William A. Grimes of the New Hampshire Supreme Court; Livingston Hall of Great Barrington, Massachusetts; Keith Mossman of Vinton, Iowa; and Cecil F. Poole of San Francisco.

The committee's objective has been to determine by what means the various federal law enforcement agencies should or could be removed or insulated from inappropriate political influence. The committee has been greatly assisted in its study by its reporter, Herbert S. Miller of the Georgetown Law Center Institute of Criminal Law. Together with Professor Miller, the committee has reviewed virtually all available literature in the field, consulted with numerous individuals who work or have worked for the relevant agencies or are otherwise familiar with the issues involved, followed congressional hearings and legislative proposals, and discussed the issues at great length in committee.

The result is a 133-page preliminary report that focuses on four major topics of concern: the Department of Justice, the office of special prosecutor, the Federal Bureau of Investigation, and the Internal Revenue Service. The proposed findings and recommendations published herewith are taken from that report. The report was submitted to the House of Delegates at the 1975 annual meeting in Montréal as an informational report. None of the recommendations has yet been considered by the House.

The committee is now reviewing and revising its report so that a final report may be submitted to the House of Delegates at the 1976 midyear meeting. In order that the final report may reflect the widest possible range of opinion, the committee seeks comments and suggestions with respect to its recommendations. Comments should be sent no later than November 5, 1975, to the Special Committee to Study Federal Law Enforcement Agencies, American Bar Association, 1800 M Street, N.W., Washington, D.C. 20036. A copy of the full report may be obtained from the committee.

I Department of Justice

A. Attorney General and the President

Findings — The Committee finds: The President should have the right to appoint his own Attorney General. The Attorney General is and should be an advisor to the President on legal matters and national policies where they are intertwined with the law. An independent Department of Justice would deny the President a legal advisor of his choice and might result in the use of White House Counsel for such purpose, thus immunizing a critical executive function from congressional oversight.

Recommendation — The committee recommends that the basic relationship between the President and his Attorney General remain unchanged, but that advice on personal and political matters be provided by sources outside the Department of Justice. The Committee opposes an independent Department of Justice.

B. Appointment of the Attorney General

1) *Findings – Politics and the Attorney General.* The Committee finds: Since World War II four of six Presidents have named as Attorney General a principal leader of a Presidential campaign in which they were elected. The close connection between partisan politics and the Office of Attorney General has seriously reduced the effectiveness of the Department of Justice, inflamed fears about the integrity of the administration of justice, and created a substantial credibility gap in the minds of the public.

Recommendation – The Committee recommends that Congress enact legislation prohibiting one who has played a leading partisan role in the election of a President from being appointed Attorney General or Deputy Attorney General. Individuals holding the position of campaign manager, chairman of the finance committee, or chairman of the national political party involved in electing the President should be among those considered to have played a leading partisan role.

2) *Findings – Importance of Attorney General* The Committee finds: The Department of Justice plays a critically important role in the federal government. It is the principal legal advisor to the President and executive branch; it is the chief prosecutor; it represents the United States in most court proceedings; it comments on proposed legislation as requested by Congress; it is the chief law enforcement agency, supervising the Federal Bureau of Investigation; it is a major fund granting agency, administering the Law Enforcement Assistance Administration; it

is the chief correctional agency of government, operating the Federal Bureau of Prisons; it plays a key role in the judicial appointment process and is an officer of the federal courts as attorney for the United States and supervisor of United States Marshals; it advises the President on pardon applications.

Recommendation – The Committee recommends that the nomination and confirmation process for Attorney General and Deputy Attorney General receive the same emphasis as appointment to the Supreme Court. The standards for appointment to these positions should be governed by the highest professional qualifications and not political reward.

C. Office of the United States Attorney

Findings – Appointment of U.S. Attorneys. The Committee finds: United States Attorneys hold an important position in the Department of Justice. They conduct most of the litigation. In exercising prosecutorial discretion they implement and help determine Departmental policy in their districts.

The Committee finds: Familiarity with practices and problems in a district contributes to intelligent exercise of the discretionary power and outweighs any advantages of having U.S. Attorneys appointed from a pool of career attorneys.

The Committee finds: The process of selecting individuals for nomination differs from district to district and may be dependent on varied factors. In general, however, partisan politics dominate the appointment process. Bar associations often play a minor role in the appointment process.

Recommendation – The Committee recommends retention of the Presidential appointment and Senatorial confirmation process for U.S. Attorneys. Nonpartisan advisory committees should be established in each judicial district for comment on the professional qualification of individuals being considered for appointment as U.S. Attorney. These committees should include representatives of the bar and some non-lawyers. They should be appointed by a panel representing the federal district court and the state or local bar association.

D. Allocating Law Enforcement Resources

Findings – The Committee finds: The Department's numerous functions and its historical development have resulted in a relatively unstructured method of allocating law enforcement resources. Basic allocation of resources has too often been determined by the exercise of unsupervised discretion at operational levels. The allocation of resources under the Attorney General's direction is essential to attain appropriate control over Department operations, help prevent improper use or abuse of law enforcement powers, and thereby gain public confidence in federal law enforcement. U. S. Attorneys and the FBI should be involved in the policy making process.

Recommendation – The Committee recommends that the Department of Justice formalize a rational system of allocating law enforcement resources with appropriate input from its operating agencies.

E. Internal Oversight

Findings – The Committee finds: The first step in restoring public confidence in the administration of justice and achieving accountability to Congress and the public is the exercise by Departmental leadership of proper oversight over its internal operations. The primary responsibility for responding to allegations concerning the abuse or misuse of law enforcement authority resides in the Attorney General.

Recommendation – The Committee recommends that there be established in the Department of Justice an Inspector General responsible to the Attorney General. The Inspector General's authority should extend to all law enforcement functions of the Department.

F. Congressional Oversight

Findings – The Committee finds: Effective congressional oversight is essential in the establishment of law enforcement resource allocations, maintenance of public confidence in the administration of justice, and as a primary method of achieving public accountability for the actions of federal law enforcement agencies. Proper congressional oversight can be a significant method of preventing and detecting the intervention of improper influences in the administration of justice. The primary need is for Congress to exercise continuous monitoring and oversight through the operations of its standing committees in the normal course of legislating, appropriating and confirming.

Recommendation – The Committee recommends that Congress strengthen the oversight function of its standing committees. Congress should use the appropriation process as a way of inducing the Department to justify funding requests in terms of its resource allocations. The confirmation process for all Presidential appointees to the Department should become a vigorous component of its oversight function.

G. Logging and Disclosure Requirements

Findings – The Committee finds: The integrity of the criminal justice process may be jeopardized by communications from individuals on matters relating to offenses under investigation or in the judicial process.

Recommendation – The Committee recommends that as to criminal matters under investigation or before the courts Department personnel keep a log on all contacts initiated from outside the Department. Such contacts should be reported in the Department of Justice. It should be a misdemeanor for intentional and knowing failure to log the contact or to make the report.

The Committee recommends disclosure to an appropriate congressional committee on request of that committee for the log. To protect the integrity of an investigation or prosecution and prevent prejudicing the rights of defendants or those under investigation, appropriate restrictions may be placed on the disclosure by the Attorney General.

H. White House Pressure for Law Enforcement Investigations

Findings – The Committee finds: White House personnel, sometimes with the approval of the President, planned and carried out activities which involved the FBI and other agencies, in a variety of law enforcement endeavors, many of them improper and politically motivated. Discussions were held in the White House which would have used the Department of Justice and the FBI to "get back at" political enemies.

Recommendation – The Committee recommends that Department of Justice personnel keep a log on all requests for the initiation of investigations or other criminal procedures emanating from the White House or Executive Office of the President. Such contacts should be reported in the Department of Justice. It should be a misdemeanor for intentional and knowing failure to log the contact or make the report.

The Committee recommends disclosure to an appropriate congressional committee on request of that committee for the log. To protect the integrity of an investigation or prosecution and prevent prejudicing the rights of defendants or those under investigation, appropriate restrictions may be placed on the disclosure by the Attorney General.

II Special Prosecutor

Findings – The Committee finds: Primary responsibility for assuring the impartial administration of justice resides in the Attorney General, including measures short of appointing a special prosecutor. Nevertheless, federal courts may be authorized to appoint a special prosecutor. Appointment of a special prosecutor by a court does not imply supervision by the appointing court over the exercise of prosecutorial discretion.

The Committee finds: The establishment of a permanent special prosecutor raises profound issues relating to the administration of justice. These include jurisdiction as to crimes and potential defendants, the power of appointment and removal, the authority to whom the permanent special prosecutor is accountable, and relationships with the Department of Justice.

The Committee finds: A special prosecutor may be necessary under certain circumstances. Institutional reform is required to avoid situations where the appointment of a special prosecutor occurs only after extreme situations develop. To assure the public of prosecutorial integrity, standards and procedures should be prescribed to guide the appointing authority.

Recommendation – The Committee recommends legislation providing for the appointment of a special prosecutor by the Attorney General under defined circumstances and standards. The Committee recommends against the establishment of a permanent special prosecutor.

The Committee recommends legislation authorizing the appointment of a special prosecutor by a special Court of Appointment. The Court could act on its own authority or upon request of the Attorney General when in its judgment the standards require such an appointment. The Committee recommends that the special Court consist of three retired senior federal circuit court judges appointed by the Chief Justice for a two-year term.

The Committee recommends that a special prosecutor appointed by the Attorney General or the special Court have the same powers as the Attorney General or a U.S. Attorney in prosecuting a case.

The Committee recommends that circumstances and standards to guide the appointing authority include the following: 1) Conflicts of interest, implications of partiality, or alleged misconduct as delineated in the ABA *Standards Relating to the Prosecution Function*; 2) Appearance of professional impropriety as delineated in Canon 9 of the ABA *Code of Professional Responsibility* ; and 3) Improper influence or obstruction of justice as defined in 18 U.S.C. 1501-1510.

The Committee recommends that the Attorney General inform the Court of Appointment of action taken in any matter where appointment of a special prosecutor was considered in accordance with the standards. A memorandum to the Court should include relevant circumstances and reasons underlying the action taken.

III Federal Bureau of Investigation

A. FBI Jurisdiction

Findings – The Committee finds: Existing federal statutes require the FBI to "detect crimes" under the supervision of the Attorney General. The FBI is further authorized "to conduct such other investigations regarding official matters under the control of the Department of Justice and the Department of State as may be directed by the Attorney General." The scope of FBI duties under these statutes needs more precise definition by the Attorney General.

The Committee finds: In the last several decades the FBI has put under surveillance and disrupted the activities of a variety of American citizens and organizations, many of whom were exercising their rights as American citizens to dissent and protest. In some instances these activities were undertaken without specific approval of the Attorney General; nor was the Attorney General always informed of such activities. These activities were subsumed under the general category of internal security.

Recommendation – The Committee recommends that the Attorney General promulgate rules and regulations to guide the FBI. These rules and regulations should be subject to the Administrative Procedures Act or a similar process which offers an opportunity for professional and citizen input.

The Committee recommends that Department of Justice attorneys exercise early and continuous supervision over the allocation of FBI investigative resources, particularly in areas involving internal security.

B. Appointment of FBI Director

Findings – The Committee finds: Appointment of the FBI Director by Presidential nomination and Senate confirmation meets the requirements of accountability and congressional oversight. These requirements (accountability and congressional oversight) would be enhanced by a periodic review of the performance of the FBI Director.

Recommendation – The Committee recommends continuation of the present method of appointment, with an additional requirement that the appointment be for a time certain, and that at the termination of this period of time a new nomination or renomination be submitted by the President for consideration by the Senate.

C. The White House and Law Enforcement

Findings – The Committee finds: High officials in the White House have engaged in law enforcement functions assigned by statute to the FBI operating under the supervision of the Attorney General. Entry into such activities by government officials not specifically authorized represents a serious departure from the rule of law.

Recommendation – The Committee recommends that employees of the executive office of the President or of the White House be prohibited from engaging in law enforcement activities unless authorized by statute. The Committee further recommends that violation of this prohibition be made a crime punishable by a term in prison.

D. Release and Dissemination of Investigative Materials

Findings – The Committee finds: The proper release and dissemination of criminal justice information among law enforcement agencies is necessary to effective law enforcement. But individual rights may be infringed if the information is disseminated irresponsibly. There is a need for legislation to provide guidelines for the release and dissemination of such information supplemented by detailed regulations issued by the Department of Justice.

Recommendation – The Committee recommends that the dissemination of such data should be prohibited except as provided by statute. The Attorney General should promulgate detailed rules and regulations relating to the release and dissemination of such data. The prohibitions should apply to state and local law enforcement agencies

receiving federal materials. A knowing violation of the prohibition should be punished as a misdemeanor.

E. Review and Oversight of FBI Operations

Findings – The Committee finds: The FBI is an essential investigative arm of federal law enforcement. There is a need for public confidence in the FBI if it is to remain a viable law enforcement agency. Constant oversight of FBI policies and operations will contribute to this public confidence and assure responsiveness to established law enforcement resource allocations.

Recommendation – The Committee recommends that review and oversight of the FBI be provided by the following recommendations previously approved by the Committee: 1) The establishment of law enforcement resource allocations; 2) The promulgation of rules and regulations delineating the scope of FBI duties; 3) The establishment of an Inspector General's office responsible to the Attorney General; 4) The close supervision by prosecutors of FBI allocation of investigative resources; 5) Congressional oversight through the appropriation, legislative and confirmation process, including review of the Director's performance by requiring a reappointment procedure at periodic intervals.

The Committee opposes outside review of FBI operations as unnecessary if the above recommendations are implemented and executed.

IV Internal Revenue Service

A. IRS Jurisdiction

Findings – The Committee finds: The IRS engaged in some politically oriented intelligence activities unrelated to the administration of the Internal Revenue laws. The potential for misuse and abuse of the IRS investigatory function could be decreased by appropriately limiting its scope of activities.

Recommendation – The Committee supports the position taken by the House of Delegates at its February, 1975 meeting to the extent that it will remove political interference from IRS operations. The adopted position is as follows:

> "Internal Revenue Service and its personnel be limited to functions, responsibilities and duties which are pertinent to the administration of the Internal Revenue laws."

B. White House Access to IRS Returns

Findings – The Committee finds: A variety of improper pressures were imposed on IRS by requests from the White House for income tax returns on particular individuals. In some instances IRS personnel improperly cooperated with individuals from the White House staff; in other cases IRS Commissioners successfully resisted requests from the White House.

The Committee finds: The integrity of the IRS and the public confidence in such integrity is essential to the continued success of voluntary reporting of tax obligations. The continued viability of the system will be threatened unless access to returns is restricted.

Recommendation – The Committee recommends legislation limiting release of returns to the White House only upon written request of the President, provided he designate a limited number of high officials of the White House staff to examine such returns. This recommendation is conditioned upon such requests being logged and reported to appropriate committees of Congress.

C. White House and Congressional Pressure for IRS Audits and Investigations

Findings – The Committee finds: The White House and congressional committees pressured the IRS to conduct investigations and tax audits on individuals and organizations. In some instances the pressures were politically motivated. Such requests jeopardize the integrity of legitimate tax audits and investigations.

Recommendation – The Committee recommends that IRS personnel keep a log on all requests for investigations or audits emanating from Congress or government officials not connected with law enforcement. All inquiries about matters under investigation should be logged. The logs should be disclosed to appropriate congressional committees. The log disclosed may be limited in scope when the Secretary of the Treasury or IRS Commissioner determines that full disclosure would prejudice the rights of individuals or groups or the effective and impartial administration of the tax laws.

D. Congressional Oversight

Findings – The Committee finds: Effective congressional oversight should be a primary method of maintaining public confidence in the administration of our tax laws and a primary method of achieving public accountability for the actions of the Internal Revenue Service. There appear to be an unusually large number of committees and subcommittees involved in IRS oversight at this time.

Recommendation – The critical need is for appropriate standing congressional committees to strengthen their continuous monitoring and oversight in the normal course of legislating, appropriating, and confirming Presidential nominees.

C. United Nations

UNITED NATIONS
ECONOMIC
AND
SOCIAL COUNCIL

Distr.
GENERAL

E/CN.4/1142/Add.2
7 October 1974

ORIGINAL: ENGLISH

COMMISSION ON HUMAN RIGHTS
Thirty-first session

HUMAN RIGHTS AND SCIENTIFIC AND TECHNOLOGICAL DEVELOPMENTS

Uses of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society

Report of the Secretary-General (continued)

		Paragraphs
PART FOUR.	THE IMPACT OF HUMAN RIGHTS OF ELECTRONIC COMMUNICATIONS TECHNIQUES	
A.	Introduction	1 - 3
B.	Principal areas of application and benefits derived from techniques in question	4 - 30
1.	Electronic data processing combined with communications ("computer communications")	4 - 20
2.	Computerized printing and related activities	21 - 24
3.	Television and radio broadcasting	25 - 30
C.	Problems affecting human rights	31 - 57
1.	Problems in the area of computer communications	32 - 50
2.	Problems concerning computerized printing and related activities	51
3.	Problems in the area of radio and television broadcasting	52 - 57
D.	Protection of human rights in the light of the new techniques	58 - 86
1.	Safeguards	58 - 83
2.	Question of draft international standards concerning the uses of electronics which may affect the rights of the person	84 - 86

PART FOUR

THE IMPACT ON HUMAN RIGHTS OF ELECTRONIC COMMUNICATIONS TECHNIQUES

A. Introduction

1. This part of the report contains a brief survey of the impact of electronic communications techniques on human rights.

2. The concept of "electronic communications techniques" covers any transfer of information from one place to another by electronic means. It includes the transfer of the printed word and the printed picture as well as the transfer of live auditory or visual messages; and the fixation and storage of such information, on audio or video tape or by other means, for future electronic transmission or retrieval. "Information", in the sense in which the word is used here, includes not only personal data relating to individuals 1/ but data and messages concerning any topic whatever. 2/

3. The impact which the rapidly evolving electronic communications techniques are having on the rights of the individual presents a vast new field for inquiry, as yet only partly explored. The present chapter, forming part of a larger report on a number of different uses of electronics, is therefore limited to a brief survey of some of the more salient aspects of this question, namely: (a) the impact on human rights of the combination of electronic data processing and communications techniques; (b) the impact on human rights of computerized printing techniques and related activities; and (c) the impact on human rights of electronic communication by way of moving picture and sound, i.e., radio and television broadcasting. 3/

1/ For computerized personal data systems see part one of this study (E/CN.4/1142 and Corr.1).

2/ The question of electronic surveillance devices has been discussed in the report on respect for the privacy of individuals and the integrity and sovereignty of nations in the light of advances in recording and other techniques (E/CN.4/1116, Add.1-4 and Add.3/Corr.1), requested in paragraph 1 (a) of General Assembly resolution 2450 (XXIII).

3/ "Electronics" has been defined as "the branch of science and technology relating to the conduction of electricity through gases or vacuum or through semiconducting materials". More narrowly, it has been defined as being concerned with

> "the design, manufacture, and application of electron tubes and solid-state devices (transistors and diodes). These devices are found in such diverse applications as home radio and television; wire or radio communications; radar ...; electric power distribution and control; x-ray production; industrial process control; and numerous aspects of national defense. The newer field of solid-state electronics has produced

(foot-note 3 continued on next page)

B. Principal areas of application and benefits derived from techniques in question

1. Electronic data processing combined with communications ("computer communications")

4. One of the more recent but increasingly important developments in the field of electronics is what has been referred to as the "marriage" of computers with communications. 4/ By this is meant, in particular, the combination of technologies which make it possible to obtain, in many cases almost immediately, information from a computer even though the person requesting it may be located in a different room, a different city, a different country or a different continent.

5. This "remote access" to the computer is obtainable by the use of so-called terminals, into which the person concerned may feed his requests or queries; they are relayed to the computer via electronic communications equipment including, as the case may be, wires, cables, micro wave, radio waves or earth satellites or combinations thereof. The reply from the computer is relayed to the terminal in the same way.

6. It is sometimes pointed out in this connexion that whereas the equipment for electronic data processing, which is a new technique, is largely in the hands of new enterprises, much of the equipment for moving the computerized data from terminal to computer and vice versa, as well as from computer to computer is in the hands of the traditional "common carriers" or utilities, such as telephone, telegraph and cable offices or companies. It is they who provide in large part the lines, circuits and modulation and demodulation equipment used. Lines for computer

---

3/ (continued)

transistors, semiconductor diodes, and other solid-state devices which are used in many of the same applications as electronic tubes ...

"A development in solid-state electronics is the integrated circuit (IC), which combines diodes, transistors, and other circuit elements and inter-connections by deposition on an insulating plate. Use of photographic methods to reduce the size of circuit components makes it possible to deposit many hundreds of transistors and other elements within an area as small as a few tenths of a square inch ...

"The transistor and the integrated circuit are credited with making possible the high-speed electronic computer." (McGraw-Hill Encyclopedia of Science and Technology, (New York, McGraw-Hill, 1971), vol. IV, p. 597).

4/ M. Greenberger, ed., Computers, Communications and the Public Interest (Baltimore and London, Johns Hopkins Press, 1971), p. xii.

communications may be leased full time or access to them may be dialed as required. For reasons of economy, circuits are often employed on a shared-use basis. 5/

7. Some "terminals" can be attached to any telephone line. This allows the user to gain access to the computer from any place, since he can utilize the pre-existing telephone network as his own computer system. 6/ World-wide data networks using land lines, underwater cables and earth satellites were stated in 1972 to be "commonplace". 7/

8. Remote access to computers is possible both for batch processing and on-line procedures. 8/ On-line interrogation of a computer by means of "console" terminals is becoming increasingly popular, however, as it enables the user to obtain a reply almost immediately and usually does not require knowledge of any "computer language" or coding system other than certain entry and exit procedures and minimal operational instructions.

9. The device most often used for slow-speed input by remote access (the technique of particular interest in connexion with remote access by individuals to information stored on electronic data processing (EDP) media) is a typewriter keyboard, modified to emit electronic signals representing the keys struck. The computer output is also received at these devices; it is typed by remote impulse in a way that makes characters appear on paper, which can be preserved by the user. It is also possible to arrange for such computer communications to carry and reproduce pictures (most commonly graphs). The output, whether writing or pictures, can also be made to appear on a lighted surface resembling a television screen. The principal mechanism used is a cathode ray tube, i.e., basically the same device as that used in home television sets. 9/

5/ The traditional "common carriers" have long been subject to regulation while regulation of the new data-processing industry is still in the early stages; the dividing line between their functions is, however, becoming somewhat blurred. Canadian Computer Communications Task Force, Branching Out (Ottawa, Dept. of Communications, 1972), vol. I, p. 127 and vol. II, pp. 3-4, 28 (hereafter referred to as Branching Out)); S. F. Furth, "Computers", in R. P. Bigelow, ed., Computers and the Law, published by the American Bar Association (New York, Commerce Clearing House, 1969), p. 33.

6/ S. Rothman and Ch. Mosmann, Computers and Society (Chicago, Toronto, Sydney, Science Research Associates, 1972), p. 87.

7/ Branching Out, vol. I. p. 126.

8/ In "batch processing", information is usually entered on punched cards or other media and accumulated before being given to the computer to be processed in "batches". Accordingly, the results of the processing are obtained at some subsequent time. "On-line" and "real-time" procedures permit direct, immediate access to and response by the computer.

9/ Rothman and Mosmann, op. cit., pp. 87-89.

10. So-called "interactive" display consoles enable the user not only to request data from the computer and refine his requests until he obtains suitable information; they enable him to "input" information on his console, which thus becomes part of the data stored in and used by the computer. They also enable him to transmit instructions to the computer relating to the solution of the problem in question. There are different types of "interactive" consoles used in the civilian context, for instance, one frequently used by engineers (who utilize these computational systems to watch processes or answers developing in the shape of a curve or markings on a map, etc.). 10/

11. Computer communications are coming to be widely used in the economic field. For example, in banking, small consoles are used by bank clerks in branch offices to check the status of an account before accepting a withdrawal slip, 11/ to verify credit balances and to update customers' accounts. Large-scale transfers of funds, both national and international, are increasingly being made via computer communications networks. 12/ Industrial enterprises are using digital communications (communications involving digital computers) to collect data from remote manufacturing plants, warehouses and sales offices and send them directly to the computer for immediate processing; similarly, they find it advantageous to disseminate reports to their remote offices over digital communications lines. 13/

12. In the social field, attempts have been made to establish computerized information systems accessible via terminals. For example, a county-wide information system, pooling data of the welfare, juvenile and adult probation, and health agencies and of the local medical centre, was projected to have ten inquiry terminals in the departments concerned, tied by telephone lines to a computer located at the civic centre. 14/

13. A beginning has also been made in introducing computer-assisted instruction via terminals into the educational process, including elementary schools as well as universities. 15/

14. In the research field, one newspaper started as a pilot operation an information bank which enables users to obtain by remote access via terminals, indexed data and summaries of information on any topic published in that paper during the past

---

10/ Ibid., pp. 89-91.

11/ Ibid., p. 86

12/ Branching Out, vol. II, pp. 63-67.

13/ Rothman and Mosmann, op. cit., p. 92.

14/ Santa Clara County, California, "The logic information system", A.F. Westin, ed., Information Technology in a Democracy (Cambridge, Mass., Harvard U. Press, 1971), p. 35.

15/ See, e.g. Edgard Faure, Felipe Herrera, et. al., Learning To Be (Paris, UNESCO, 1972), pp. 125-127.

several years; the computer also indicates related headings under which additional information might be found. 16/

15. Elsewhere, work was in progress in 1970, aimed at establishing remote access among libraries to information concerning such matters as acquisition, cataloguing and lending of books. The country was to be divided into five districts, each centred on a university; each library in that district was to be connected "on-line" with the university and the region was to be connected via a telecommunication network to a central library computer. 17/

16. A number of remote-access information systems are being developed in international organizations, for example, the Integral Scientific Information System (ISIS) of the ILO.

17. Much work is being done with a view to setting up satisfactory systems for translating into machine-readable form laws and court decisions (and in some cases legal literature) and to make possible on-line remote access to the computer on questions of law. Thus in Australia, a number of working groups have been set up consisting of federal and state legal officials, and of private legal practitioners in some cases, to study the implication of the computerization of legal and other official information; the expectation being that such computerization will lead to a more scientific approach to law, greater certainty in ascertaining the law and, generally speaking, better administration of justice. 18/ Sweden has undertaken the computerization, on a terminal-based system, of laws and other statutes published in the official Swedish Statute Journal (SFS) and of decisions of the Supreme Administrative Court and the two Administrative Courts of Appeals. 19/ Other such projects have been reported in the Federal Republic of Germany, 20/ the United Kingdom 21/ and the United States. 22/

16/ The New York Times. Cf., e.g., A. N. Feldzamen, The Intelligent Man's Easy Guide to Computers (New York, David McKay Company, 1971), p. 46 (hereafter cited as: Feldzamen, Easy Guide).

17/ "Information Systems in the Administration", information forwarded by the Government of Sweden on 21 August 1973; the system was stated to be in operation on an experimental basis.

18/ Information forwarded by the Government of Australia on 3 May 1973.

19/ "System for legislative procedure and case law", information forwarded by the Government of Sweden on 21 August 1973.

20/ J. Fabry, "Developing a legal information system for the Federal Republic of Germany", work paper submitted to the Abidjan World Conference on World Peace Through Law (Abidjan, Nigeria, 26-31 August 1973).

21/ B. Niblett and N. Price, "On-line interrogation of Acts of Parliament", Intergovernmental Bureau for Informatics, IBI-ICC, Papers of the First World Conference on Informatics in Government, held in Florence, Italy, 16-20 October 1972 (hereafter cited as IBI-ICC Papers), part 3, pp. 902-905.

22/ A. Kaltman, "Computer applications in American State Government", IBI-ICC, Papers, part 2, p. 416; J. F. Horthy, Jr., "Use of the computer in statutory research and the legislative process", in R. P. Bigelow, ed., Computers and the Law, publication of the American Bar Association, Standing Committee on Law and Technology (New York, N.Y., Commerce Clearing House, 1969), pp. 53-60.

/...

18. The intention is to make such legal information more easily and widely available. Some discussion has arisen over the respective merits of computer-storage of abstracts as against the full text of legal materials, weighing usefulness and costs. 23/

19. Consoles (CRTs) are also beginning to be used for transmitting actual news stories to newspapers. This process, which was introduced largely to mesh with computerized printing of newspapers (see below, section B.2., Computerized printing and related activities) has been described as follows:

> "When correspondents' stories reach /the/ central offices /of a large news agency/, they are now fed directly into computers. Seated next to their CRTs, wire-service editors can order the computer to display on-screen a list of all stories filed during the previous 24 hours. Another command can call up the text of a story, which is then seen on the screen in segments of up to 31 lines at a time. As the editor electronically rolls the story forward, he can maneuver a lighted blip called a 'cursor' to make changes in the copy. If he wants to revise a paragraph, he presses buttons that tell the cursor to remove that block of text. Then he types in his own version on the screen. The edited story is returned to the computer and sent to subscribing papers. ...
>
> "The full effects of these alterations depend on the newspapers that get the copy. Without special receiving equipment, wire-service stories still creep in over teletype machines at the maximum rate of 66 words a minute. Papers that have invested in new machines are a long leg up on competitors; high-speed printers can receive wire stories at 1,050 words a minute, a major advantage at deadline time." 24/

20. A number of serious studies envisage the possibility of remote access computing facilities being brought into the individual home in the not too distant future in the same way as television. 25/

2. Computerized printing and related activities

21. Electronic technology is also having an impact on an older medium of communication, namely, printing. This new production method is being used both in newspaper publishing and in book publishing. Automated systems have been devised

---

23/ See, e.g., J. F. Horty, Jr., "Use of computers for law office research", in Bigelow, op. cit., pp. 46-50; Fabry, op. cit.

24/ Time Magazine (New York, N.Y.), 17 December 1973.

25/ E.g., Branching Out, vol. II, p. 63; P. Baran, "The future computer utility" in I. Taviss, The Computer Impact (Englewood Cliffs, N.J., Prentice-Hall, 1970), p. 83.

in which the computer is programmed to generate input media such as magnetic tape for use in type-composition machines. The type is set by a photographic process. 26/ This method of printing is very fast, has a number of technical advantages and requires less labour since photo-typesetting, for example, eliminates the need for hand composition.

22. Computer printing can, moreover, be combined with computer-assisted composition, editing and revision of texts. This technology, whereby changes can be made directly onto the easily erasible magnetic tape, eliminates much of the retyping involved in drafting. It also eliminates the work and cost involved in resetting type after galley proofs have been corrected, since the tape serves as the "galleys" and the actual "printing" takes place only after the tape has been finally proof-read and corrected. 27/ Where it is desired to keep a record of the different stages through which the draft has passed, computer print-outs may be made at each stage. It is considered that computerized drafting, in combination with photo-typesetting, considerably reduces production costs, for example, in the area of legislative drafting and printing. 28/

23. These drafting techniques can be employed by remote access, through the use of terminals. 29/

24. News stories computer-edited in the newsroom (see above, para. 19), may be transmitted by computer to the printing plant. It has been reported that computers are able to set type photographically at 300 lines a minute and partially control the operation of the printing presses. These changes make it possible for last-minute news items to be included in a newspaper 15 minutes before press time, as compared to the hour required previously. 30/

3. Television and radio broadcasting

25. Radio broadcasting, which started about 50 years ago and spread rapidly all over the globe, was given additional importance by the invention of the transistor radio after the Second World War.

26/ J. F. Horty, "Use of the computer in statutory research and the legislative process", in Bigelow, op. cit., p. 59; J. C. Lyons, "Integrated research and publishing", ibid., p. 60; Time Magazine, 17 December 1973; R. L. Chartrand, "Rational change: the promise and the process", in R. L. Chartrand, ed., Computers in the Service of Society (New York, Pergamon Press, 1972), p. 7.

27/ P. Armer, "Computer applications in industry and services", in I. Taviss, The Computer Impact (Englewood Cliffs, N. J., Prentice-Hall, 1970), p. 51; see also references in preceding foot-note.

28/ "System for legislative procedure and case law", information forwarded by the Government of Sweden on 21 August 1973.

29/ R. L. Chartrand, "Rational change: the promise and the process", in R. L. Chartrand, ed., Computers in the Service of Society (New York, Toronto, Pergamon Press, 1972), p. 7.

30/ Time Magazine, 17 December 1973.

26. Radio broadcasting had made it possible for people in cities and towns as well as in more isolated rural areas, as long as they were served by electricity, to be quickly informed of national and international news and to have access to music, dramatic performances and educational and entertainment programmes frequently unavailable to them by any other means. The development of short-wave and other special-wave broadcasting enabled many listeners, moreover, to tune in not merely to a few relatively near-by stations but, depending on their location, to programmes from half a dozen or more countries, some of them nearly half-way around the globe.

27. The subsequent invention of the transistor radio, which runs on batteries, has brought radio reception to areas not as yet served by electricity. 31/ It has also made possible the production of very small, inexpensive radios (suitable at least for local reception) and thus extended even further the circle of people who can be reached by radio broadcasts.

28. A new dimension was added with the introduction of television broadcasting, which added direct, visual impact to the broadcast. It made possible entire new categories of programmes, for example, travelogues showing the natural beauty, art treasures or living conditions of distant countries; instructional television utilizing pictures, drawings, live demonstrations, etc., to facilitate the learning process; theatrical performances and other entertainment spectacles from various cultures; current events; or sports events. Mass production of television sets and the accompanying reduction in their price has brought television within the reach of relatively large audiences, quite apart from communal reception.

29. A further dimension was added to this with the use of communications satellites for radio and, particularly, television broadcasting. 32/ Such broadcasts are currently beamed via satellites to earth stations, to be relayed to individual television sets. Advances in technology are, however, expected to make possible in the near future the reception of television broadcasts from satellites directly into community receivers, without any need for earth relay stations; later on, directly into home receivers augmented by relatively inexpensive equipment; and ultimately, directly into ordinary, unaugmented home receivers. 33/

31/ Battery-operated radios were in existence before the invention of transistor radios but, due to their relatively high price, large size and fragile components were generally beyond the reach of people in the lower income groups and in remote areas.

32/ The bulk of the traffic carried by communications satellites consists, however, of individual rather than broadcast messages, including computer data.

33/ See document A/AC.105/83, paras. 15-16, 69.

30. The actual and potential impact of radio and television in the areas of education, economic and social development and culture have been the subject of numerous studies prepared under the auspices of UNESCO. These include, among others, Radio Broadcasting Serves Rural Development; 34/ John Maddison, Radio and Television on Literacy. A Survey of the Use of the Broadcasting Media in Combating Illiteracy Among Adults 35/ Radio and Television in the Service of Education and Development in Asia; 36/ Adult Education and Television; 37/ I. Waniewicz, Broadcasting for Adult Education. A Guidebook to World-Wide Experience; 38/ P. Fougeyrollas, Television and the Social Education of Women; 39/ Television for Higher Technical Education of the Employed. A First Report on a Pilot Project in Poland; 40/ Communication in the Space Age. The Use of Satellites by the Mass Media; 41/ Broadcasting from Space; 42/ W. Schramm, Communication Satellites for Education, Science and Culture; 43/ and A Guide to Satellite Communication. 44/ Reports by UNESCO relating in part to this question were submitted to the twenty-eighth session of the General Assembly (A/9227) and the thirtieth session of the Commission on Human Rights (E/CN.4/1144).

34/ UNESCO, Reports and Papers on Mass Communication, No. 48 (1965).

35/ Ibid., No. 62 (1971).

36/ Ibid., No. 49 (1967).

37/ Ibid., No. 50 (1967).

38/ UNESCO, Paris (1972).

39/ Co-edition UNESCO/National Institute of Adult Education, England and Wales (1966).

40/ UNESCO, Reports and Papers on Mass Communication, No. 55 (1969).

41/ UNESCO, Paris, 1968, 200 pp.

42/ UNESCO, Reports and Papers on Mass Communication, No. 60 (1970).

43/ Ibid., No. 53 (1968).

44/ Ibid., No. 66 (1972).

C. Problems affecting human rights

31. As has been the case with other technical advances of great usefulness and a multitude of diverse applications, the rapid expansion of electronic communications techniques is creating new situations capable, under certain conditions, of affecting adversely some of the fundamental rights and freedoms proclaimed in the Universal Declaration of Human Rights. Such situations are not necessarily the result of abuses; they may also arise as the unintended, little-noticed by-products of otherwise benign and even beneficial developments. An awareness of potential problems in this area may make it possible to forestall their occurrence.

1. Problems in the area of computer communications

32. The principal problems affecting human rights that have so far been noticed in the area of computer communications concern access to information stored in computers; the integrity and quality of such information; and control over computer communications. Access to and the integrity and quality of information are issues which touch on the right proclaimed in article 19 of the Universal Declaration of Human Rights and article 19 of the International Covenant on Civil and Political Rights. Control over computer communications may in some situations have a bearing on the right to self-determination of peoples as enunciated in article 1 of the latter as well as in article 1 of the International Covenant on Economic, Social and Cultural Rights.

33. The relevant texts read as follows:

Article 19 of the Universal Declaration of Human Rights

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

Article 19 of the International Covenant on Civil and Political Rights

"1. Everyone shall have the right to hold opinions without interference.

"2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

"3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

"(a) For respect of the rights or reputations of others;

"(b) For the protection of national security or of public order (ordre public), or of public health or morals."

Article 1, paragraph 1, of the International Covenant on Economic, Social and Cultural Rights and the International Covenant on Civil and Political Rights

"1. All peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development ..."

34. As for the question of access to computerized information, it will be recalled that in Part One of the present report (E/CN.4/1142), which dealt with personal data, emphasis was placed on ensuring confidentiality so as to protect the privacy of the individual. By contrast, one of the problems with information of a non-personal nature is that of finding ways of making these materials easily accessible to persons wishing to consult them. While computer communications are employed in many fields precisely for the purpose of making information more widely and more rapidly available, there are some uses where problems may develop unless proper arrangements are made.

35. Problems may arise, for example, in connexion with the storage on magnetic tape, discs, punch cards or similar media, of information that previously has been commonly available for consultation in government offices, archives, libraries, newspaper offices or institutions of higher learning; e.g. statistical or scientific papers, documents, manuscripts, clippings, dissertations, and hard-to-obtain books. Computerization may be limited to indices of the materials available or it may provide abstracts (where this is possible) or the complete data or texts concerned. Problems of access to such information may arise in particular where abstracts and complete data and texts are stored on EDP media, if following computerization the materials, for one reason or another, can no longer be consulted in their original written or printed form. 45/

36. This problem has been discussed in some detail in Sweden, where unrestricted access to official documents is granted to the public under the Freedom of the Press Act, which forms part of the Constitution (some exceptions relating, e.g., to foreign affairs, defence and police matters and the protection of individual privacy, are specified in the Secrecy Act). A Royal Commission on Publicity and Secrecy of Official Documents submitted a report in 1972 which, although largely concerned with protecting the privacy of the individual, 46/ did address itself to the problem of access to some extent.

45/ Cf., e.g., Guy Braibant, "La protection des droits individuels au regard du développement de l'informatique, "Revue internationale de droit comparée, vol. 23, No. 4 (October-December 1971), p. 810, forwarded by the Government of France on 5 February 1973 (hereafter referred to as Braibant, "La protection"); also Aimé François, "L'informatique et l'administration", xx^{e} Congrès International des Sciences Administratives, Rome, 6-11 Sep. 1971 (Brussels, Institut International des Sciences Administratives, 1973), pp. 62, 64, forwarded by the International Institute of Administrative Sciences on 6 February 1973 (hereafter referred to as François, "L'informatique").

46/ See document E/CN.4/1142, paras. 62, 87, 96.

37. The report pointed out, on the one hand, that the rules governing official "documents" have, in practice, been interpreted by the Supreme Administrative Court of Sweden to be applicable to magnetic tapes; and that the reasons adduced by the Court indicate that the rules also apply to other media used in electronic data processing, such as punch cards and discs. 47/ This means that in Sweden computerized official data should be as accessible to the public as the data contained in official documents.

38. On the other hand it has been pointed out that, nevertheless, information stored on magnetic tapes or other electronic data processing media tends to be less available than it would be if collected in documents:

> "ADP-media cannot be read without the help of a computer. This requires much more work and involves higher costs than reading a document and implies in reality that the access to information for the public can be impaired through computerization." 48/

39. The question of accessibility to computer-stored information has also been raised in the context of research materials. It has been stated, for example, that a large proportion of scientific data is currently not available in printed form, but is only stored in computers, thus complicating access to the information. Apprehension has been expressed, moreover, that the practice of substituting computer-storage for duplication processes like printing may spread to other areas of knowledge. 49/

40. Arguments favouring such a development include the following:

> "We need to substitute for the book a device that will make it easy to transmit information without transporting material, and that will not only present information to people but also process it for them, following procedures they specify, apply, monitor, and, if necessary, revise and reapply. To provide those services, a meld of library and computer is evidently required ... In thinking about procognitive systems - systems to facilitate man's interaction with transformable information - we should be prepared to reject the schema of the physical library - the arrangement of shelves, card indexes, check-out desks, reading rooms, and so forth. That schema is essentially a response to books and to their proliferation ... We should be prepared to reject the schema of the physical book itself, the passive repository for printed information ... It no longer seems likely that we can organize or distill or exploit the corpus /of knowledge/ by passing large parts

---

47/ Summary of report (SOU 1972:47) and draft Data Act submitted by the Commission on Publicity and Secrecy of Official Documents (hereafter referred to as Sweden, Computers and Privacy), forwarded by Government of Sweden on 21 August 1973.

48/ J. Freese, "The Swedish Data Act", Current Sweden, No. 4 (July 1973), p. 2, forwarded by the Government of Sweden on 21 August 1973; also Sweden, Computers and Privacy.

49/ K. Czernetz, "Technologie and Menschenrechte", Revue de droit international (Geneva), vol. 51, No. 2 (April-June 1973), pp. 135-143.

of it through human brains. It is both our hypothesis and our conviction that people can handle the major part of their interaction with the fund of knowledge better by controlling and monitoring the processing of information than by handling all the detail directly themselves..." 50/

41. Elsewhere it has been pointed out that, for instance, books containing reference material that changes significantly in a short time might no longer be printed if the information could be supplied by an information utility, 51/ i.e. broadly speaking, a computer-based network for retrieving information stored on electronic data processing media, accessible to anyone at a small fee.

42. The question has also been raised of what possibilities of access, if any, there may be to the large stores of computerized information that are being accumulated by economic enterprises. 52/

43. Attention has also been drawn to the fact that whereas some recourse procedures do exist which make it possible to appeal against a refusal to grant access to one's own personal data, there is no recourse where access is refused to computerized information on any other subject. 53/

44. Access to the computer via terminal permits, potentially, extensive monitoring. Computer procedures originally developed to help ensure the security and integrity of computerized data, can be used to identify and register each terminal calling and each inquiry and reply made. 54/

45. As for the question of the integrity of information that is made available by means of computer communications, attention has been drawn to, among other factors, the ease with which information stored on data processing media may be up-dated or altered; and the potential information monopoly which may be created, in certain circumstances, by reliance on a central computer.

50/ J. C. R. Licklider, "Libraries and information", in Taviss, op. cit., pp. 260-261.

51/ Armer, op. cit., p. 51.

52/ Cf. Braibant, "La protection", pp. 800, 809-810, concerning access to computerized information held by large private corporations.

53/ François, "L'informatique", pp. 62, 64.

54/ Cf., e.g. A. G. Oettinger, "Communications and the national decision making process", in M. Greenberger, ed., Computers, Communications and the Public Interest (Baltimore, Johns Hopkins Press, 1971), pp. 74-91; G. Self[illegible]ge, "Social responsibility and computers", in J. M. Beshers, ed., Computer Methods in the Analysis of Large-Scale Social Systems, second ed. (Cambridge, Mass. and London; M.I.T. Press, 1968), pp. 214-215.

46. As to the first point, the very ease with which data recorded on discs, magnetic tape, etc., may be corrected, updated or erased 55/ makes these media particularly useful for many business needs; as indicated previously, it also makes computerized drafting and editing an efficient technique for certain purposes. At the same time, however, exclusive storage of information on such media facilitates the manipulation of index entries, summaries, statistical data, etc., compared with printing and other duplicating processes. Magnetic tape is, moreover, easily destructible by fire and easily spoiled by inexpert handling.

47. As to the danger of creating a potential "information monopoly", there has been considerable discussion whether computer communications tend to "centralize" or "decentralize" information. It has been pointed out, on the one hand, that computer communications help to make data easily available and thus facilitate a rapid diffusion of information; and, on the other, that they facilitate centralized control over what information is stored and available for consultation and diffusion. 56/ Centralization of input is the favoured technique due to the fact that centralized processing and transmission facilities are generally considered to be more efficient than smaller facilities, both technically and financially. 57/

48. Closely related to the question of the integrity of information is the question of its quality. It should be kept in mind that information available for retrieval by computer communication can be no better than the quality of the material originally processed and the quality (and relevance to the user's inquiry) of the preparatory steps, referred to in parts one and two of the present paper, 58/ required for all electronic data processing. 59/

49. Another problem, potentially related, which is mentioned by many writers in the field is that of "information overload", i.e. the capacity of computer communications to furnish the inquirer with far greater volumes of information, often trivial, than he can absorb and utilize within the time span at his disposal

---

55/ Information stored on magnetic tape can easily be erased and the tape re-used. To up-date individual entries on magnetic tape it is, however, less complicated and hence customary to make a new tape rather than correct the old one; as a matter of policy three "generations" of such tapes may be preserved to permit comparison or replacement when necessary. In the case of discs, which are more expensive than tapes, changes are usually entered directly onto the disc in question, as discs allow direct ("random") access to the item desired. Cf., e.g., What the manager should know about the computer, Dun and Bradstreet Business Series, No. 7 (New York, Dun and Bradstreet, Inc., Education Division, 1970), pp. 104-105.

56/ Cf. e.g., François, "L'informatique", pp. 64-65; I. de Sola Pool, S. McIntosh and D. Griffel, "Information systems and social knowledge", in A. Westin, Information Technology in a Democracy (Cambridge, Mass., Harvard University Press, 1971), p. 248 (hereafter referred to as Westin, Information Technology).

57/ Cf., Baran, op. cit., pp. 86-89.

58/ E/CN.4/1142, paras. 16 to 23 and E/CN.4/1142/Add.1, paras. 1 to 8.

59/ Feldzamen, Easy Guide, pp. 28, 49 ff.; F. W. Horton, Jr., Reference Guide to Advanced Management Methods (New York, Advanced Management Association, Inc. 1972), p. 109.

and the resulting need to pre-select the type of information that is to be transmitted. 60/

50. As for control over computer communications and the potential impact of such control on sovereignty and self-determination, mention was made in paragraph 6 of the fact that the equipment for electronic data processing is largely in the hands of new, mostly unregulated enterprises while the equipment for moving the data from computer to user is largely in the hands of the traditional publicly-owned or regulated "common carriers" (although some overlapping activities are starting to develop). This situation is considered by some to complicate regulatory efforts to some extent, particularly where, as is sometimes the case, the data-processing equipment is foreign-owned or even physically located outside the borders of the country receiving information. The point has been made that, where used for information retrieval and dissemination, educational processes and entertainment, data processing and data bank services convey cultural values and care must be taken to ensure that users have "a choice of materials including a sufficient volume of domestic sources". 61/ Implications for national sovereignty have also been pointed out where data relating to natural resources are processed and stored outside the country concerned. Attention has, moreover, been drawn to the fact that facilities located physically outside the country concerned are not subject to the latter's laws, e.g. laws relating to security or liability. 62/

2. Problems concerning computerized printing and related activities

51. While computerized printing is considered to have many technical advantages, some of which have been referred to in paragraphs 21-24, above, apprehension has been expressed that the very heavy capital outlays required for the original investment in electronic equipment will make it impossible for the smaller, independent newspapers and publishing houses to continue to function, thus accelerating current trends towards centralization in these fields and leading to the establishment of press monopolies. Such a development, it is feared, would thus jeopardize the freedom of opinion and expression as proclaimed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (see above, paragraph 35) in that it would make it very difficult for smaller groups and individuals to maintain or establish their own presses or newspapers or otherwise gain access to publishing media. Attention has been drawn to the particular importance of the continued existence of independent printing establishments in view of the monopoly or near-monopoly conditions that sometimes exist, due to technical and cost factors, in respect of the other mass media, i.e., radio and television. 63/

60/ Cf., e.g., R.A. Bauer, "Social planning", in Taviss, op. cit., pp. [illegible] Feldzamen, op. cit., p. 28, 165 [illegible] H. A. Simon "Designing organizations for an information-rich world", in Greenberger, op. cit., pp. 44-47; Ackoff, "Management misinformation systems", in Alan McKenney, Information Technology (Cambridge, Mass., Harvard University Press, 1971), pp. 265-266.

61/ Branching Out, vol. I, pp. 142-143, 148-150.

62/ Ibid., vol. I, pp. [illegible].

63/ Cf. e.g., Czernetz, op. cit., pp. 135-137.

3. Problems in the area of radio and television broadcasting

52. Potential problems in the area of radio and television broadcasting are foreseen largely in connexion with broadcasting via communications satellites. Despite the great benefits which are expected from the use of this developing technology, fears have been expressed that satellite broadcasts, especially once they can be heard and seen directly on home sets without any need for passing through earth relay stations of the receiving country, might be abused to spread false news or indoctrinate unsuspecting audiences; or that, particularly due to the strong impact of television on the viewer, the direct and indiscriminate onslaught of modern cultures on traditional cultures might serve to destroy the latter rather then stimulate them to evolve and adapt to new conditions.

53. This matter has been discussed in the Secretary-General's study entitled "Respect for the integrity and sovereignty of nations in the light of advances in recording and other techniques". 64/

54. Reference to the impact of television was also made in the report on the impact of scientific and technological developments on economic, social and cultural rights submitted by UNESCO to the Commission on Human Rights at its thirtieth session. 65/

55. One particular problem in the area of broadcasting is that of subliminal messages conveyed by radio or television. Examples available pertain to television. The technique consists in projecting on television repeatedly, for fractions of a second, "messages by light or sound so quickly and faintly that they are received below the level of consciousness". 66/ The method has been used, both experimentaly and commercially, as a means of advertising, to stimulate the demand for a given product. It has also been used experimentally to test its effectiveness in suggesting opinions (e.g., as to whether the face of a person visible on a screen expressed happiness or unhappiness) and in suggesting a given thought. Apprehension has been expressed that such methods could be used to influence people not only in the area of merchandising but also in the area of politics.

> "... /a/ new technique ... projects photos many times on a screen for less than 1/16 second during the performance of a moving picture. Due to the shortness of time, the contents of such photos are not taken notice of consciously; yet they exert a decisive influence on people as has been

---

64/ E/CN.4/1116/Add.3 and Add.3/Corr.1. This document forms part two of the study entitled "Respect for the privacy of individuals and the integrity and sovereignty of nations in the light of advances in recording and other techniques" (E/CN.4/1116 and Addenda 1 to 4) requested in para. 1 (a) of General Assembly resolution 2450 (XXIII).

65/ E/CN.4/1144.

66/ Cf. Alan Westin, Privacy and Freedom (New York, N. Y. Atheneum, 1967), p. 279.

proved by experiments. This constitutes an immense danger in political and other respects." 67/

56. Subliminal techniques have also been described in the following terms:

"There are subliminal and brain-washing techniques by which the subconscious of the individual is invaded and his thoughts or personality influenced without his consent. These influences can be smuggled in past the customs of the senses. Methods of which I am aware include ultrasonic waves. These are inaudible to the conscious senses, like the 'silent' dog-whistle inaudible to man. At sonic frequencies just beyond the threshold of normal hearing an insidious and persistent silent message can, at unsuspecting moments, get through to the subconscious - like the signal of an unfamiliar radio-station impinging on a neighbouring wave-band. Similarly subliminal messages can be concealed in films or television programmes. Of course, such means are banned but anyone sufficiently ingenious, or some central authority seeking to indoctrinate, could succeed ... Unless one could investigate at the point of preparation, it would be difficult to establish this intrusion because by very definition the conscious senses would not recognize it; it would be subliminal at the receiving end, and therefore undetectable." 68/

57. Experiments have also demonstrated that it is possible to hypnotize persons via television. 69/

67/ Council of Europe, Consultative Assembly, Report on human rights and modern scientific and technological developments (Rapporteur: Mr. Czernetz), document 2326 of 22 January 1968, p. 4; see also commentary on article 8 (1) accompanying Belgian draft law dated 26 January 1972; forwarded by the Government of Belgium on 15 February 1973.

68/ Ritchie-Calder, "Technology and human rights", paper prepared for the Assembly for Human Rights, Montreal, 22-27 March 1968.

69/ Cf. e.g., Westin, Privacy and Freedom, p. 297.

D. Protection of human rights in the light of the new techniques

1. Safeguards

Computer communications

58. Electronic communications techniques being, like the computer uses discussed in part two of this report, 70/ a new and rapidly developing branch of technology, their full impact on human rights, positive and negative, may not as yet be fully apparent. Moreover, comparatively little attention seems to have been focused so far on the question of protecting human rights in that area. Whereas the benefits of the techniques discussed are evident, the problems and potential problems are only just beginning to be identified and to some of them there appear to be no easy answers.

59. The safeguards which may be required to protect human rights in the area of computer communications cannot be discussed entirely apart from safeguards required in certain specialized areas of computer use, such as computerized personal data systems and the use of the computer in policy-making and management processes. Some of the protective measures referred to earlier on in the present report 71/ in connexion with those topics are also relevant in the broader field of computer communications. This applies, for example, to such matters as physical and technical safeguards to protect computerized data against alteration by unauthorized persons; to some professional safeguards, such as the introduction of codes of ethics; the need, in many cases for the user to know the computer programme in order to be aware of the criteria that were applied in processing the data he is receiving; or the concept of a "computer utility", which would enable various organizations and the public at large to have access to computing and retrieval facilities at moderate fees (or in some cases free of charge). The importance of access to advanced computer techniques has been referred to in connexion with the use of the computer in policy-making and management processes; 72/ access to information stored on electronic media is of comparable importance.

60. In working out protective measures in the area of computer communications, a basic and viable distinction may have to be drawn, however, between computerized personal data systems, which should be obliged to preserve the privacy of the individual; systems which deal not with personal data but with data serving specific governmental or private requirements for information, be they administrative, economic, financial or other; and systems designed to provide access to information for members of the public on the same basis as libraries, archives, non-restricted governmental offices and similar collections.

70/ E/CN.4/1142/Add.1, paras. 1 to 92.

71/ Cf. E/CN.4/1142, and Corr.1, paras. 121 to 320, and E/CN.4/1142/Add.1, paras. 74 to 92.

72/ See E/CN.4/1142/Add.1 paras. 68, 85-89.

60a. The paragraphs below relate primarily, though not exclusively, to the last-mentioned group and relate largely to the questions of access to information, the quality and integrity of information and control over computer communications.

61. Access to materials stored on EDP media may in some cases be assured by regulatory measures. Thus, under the conditions prevailing in Sweden (see above, paras. 36-37) the Swedish Royal Commission on Publicity and Secrecy of Official Documents in 1972 proposed amending the rules governing EDP records to provide that wherever they dispose of the means to do so, governmental authorities are to make computerized information available to the public in readable form (e.g. by print-out or displayed by means of a cathode ray tube); with the transfer of such information on-line to another computer to be possible but not compulsory. 73/

62. It has also been suggested, in professional literature on this subject, that where a governmental authority, for financial reasons or lack of space, decides to preserve data only by storage on EDP media, it should be bound to make such information accessible to persons requiring it, either free of charge or at charges no higher than the cost of the publications in which information of that kind was previously published. 74/

63. The question of whether or not to destroy copies of published materials, once the information in question has been stored in its entirety on EDP media, should be decided depending on the particular materials in question, always making sure that computerization serves to facilitate and not to restrict access to information.

64. Also for the purpose of protecting the quality and integrity of information on EDP media, in view of the ease with which such information may be altered or destroyed and the possibility of error during processing, care should be taken to establish a coherent policy for preserving the original documents and other texts or data on which the stored information was based, and for continuing to make these materials accessible to readers. 75/

65. On the question of centralization or decentralization of computing facilities it has been suggested that, at least in the area of computing facilities designed for academic and research purposes, the establishment of a single over-all national data centre would neither be desirable, due to its implications for the quality of the processing done, nor necessary in order to achieve co-ordination:

73/ "Computers and privacy" summary of report (SOU 1972. 47) and draft Data Act; information forwarded by the Government of Sweden on 21 August 1973.

74/ Braibant, "La protection", p. 810.

75/ Keeping in mind any necessary safeguards where the materials involve personal data, as mentioned, e.g., in part one of this report (E/CN.4/1142), paras. 111-117.

" ... at many points in the initial processing of acquisitions, quite specific substantive and methodological expertise is extremely important. Even for routine 'housekeeping' functions involved in subsequent physical storage and maintenance of data, some minimal data-specific familiarity is useful. In short, repository workers require deeper understanding of the materials they handle than the conventional librarian does even for classifying books. However, not only are the required trained personnel in short supply, but it would also be undesirable to locate those available in a single place, even if this could be done.

More important is the fact that the advance of telecommunication renders the concept of a decentralized network of data repositories entirely feasible. Such a national net of service facilities, distinguished by nodes of methodological and topical specialization, would permit the intellectual functions associated with data-assembly to be carried out with resources on site in the appropriate repository. At the same time, the facility would be on line for occasional queries from other repositories in the system and could be approached readily through any facility in the network". 76/

66. Proposals for enforceable codes of ethics have been mentioned in part one of this report, in the context of safeguarding the integrity of computerized personal data systems. Such codes should, of course, extend to computer communications relating to any other topic. It has been pointed out that, to be effective, the codes would have to be applicable not only to computer personnel proper but also to other categories of persons involved directly or indirectly with computer communications, including persons at the policy-setting level and general administrators. Also where, for instance, government authorities are having data processed or maintained by private firms, the employees of the latter should equally be subject to the code, as should the producers of computer "hardware" and "software . 77/

67. The British Computer Society's Code of Ethics, while not addressing itself specifically to the questions of the quality and integrity of information processed, stresses the need for professional competence and ethical behaviour (section II); it also contains "notes for guidance" which provide that members of the Society should have regard to "the effect of computer based systems, in so far as these are known to them, on the basic human rights of individuals whether within the organisation /they serve/, its customer or supplier or among the general public". 78/

76/ Committee on Information in the Behavioral Sciences, Communication Systems and Resources in the Behavioral Sciences, Publication 1575 (Washington, D.C., National Academy of Sciences 1967), p. 31.

77/ Braibant, "La protection", pp. 808-809. François, op. cit., pp. 66-69.

78/ The British Computer Society Code of Conduct (approved by the Council of that organization on 17 February 1971), sect. III point 2.12, appendix N of Report of the Committee on Privacy (Cmnd. 5012), forwarded by the Government of the United Kingdom on 26 July 1972.

68. In addition to codes of ethics, the need has been stressed for protective legislation but, so far, only a few relevant examples are available.

69. The Swedish Data Act of 1973 established a new crime of "data trespass", which included the unlawful altering or erasing of records for computer processing. Offenders were made subject to a fine or to two years' imprisonment (if the offence in question is not otherwise covered by the Penal Code). 79/ Attempted data trespass was also made punishable.

70. The Data Protection Act of the State of Hessen in the Federal Republic of Germany provides that information covered by "data protection" shall be "obtained, transmitted and stored in such a way that /it/ cannot be ... altered .. or destroyed by an unauthorized person. This shall be ensured by appropriate staff and technical arrangements". 80/

71. There is considerable discussion of questions concerning licensing and other regulatory steps for the computer communicatic s industry but this relates largely to rate structure, the prevention of monopolies and other economic and administrative issues. The report of the Canadian Computer/Communications Task Force referred to previously recommended, for example, that organizations offering data services commercially to customers through telecommunications facilities, with terminals on remote premises, should be required to register with an appropriate body and file information on their corporate structure and on their data services. The Task Force suggested more specifically the establishment of a Registrar of National Computer/Communications networks. 81/ Although licensing is being used in some countries in respect of computerized personal data systems, it is too early to tell, from the materials at present available, whether licensing could or should be used more generally, to protect access on a non-discriminatory basis to data processing services to remote retrieval facilities and to information that would be open to the public but for storage on EDP media; or to protect the integrity of the information stored on EDP media.

79/ J. Freese, "The Swedish Data Act", Current Sweden, No. 4 (July 1973), p. 6; forwarded by the Government of Sweden on 21 August 1973. The article points out that this provision covers a wider field than the protection of privacy (which is a central purpose of the Act). See also E/CN.4/1142, paras. 87, 96-97, 306.

80/ Data Protection Act of 7 October 1970, section 2. This law deals largely with the protection of personal data but also refers to "data and stocks of data containing no individual details concerning natural or legal persons and permitting no such details to be inferred" (section 5 (3)).

81/ Branching Out, vol. I, pp. 140 and 206, recommendation 23. As envisaged in that study, the Registrar would have no discretionary power to refuse registration of any organization which provided the necessary information. Ibid., pp. 185-186.

72. Except for the area of computerized personal data, hardly any information is available as yet concerning effective remedies where access is refused to information stored on EDP media.

73. To the extent that computer/communications utilize common carrier telephone lines and cables, existing safeguards against wiretapping and eavesdropping could be expected to apply to computerized information moving over such lines.

74. Attention may also be drawn to existing legislation dealing with "common carriers" which may specify, for example, that it is unlawful for such carriers "to make any unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services ... or to ... give any ... unreasonable preference or advantage to any /parties/". 82/

75. As for control over computer communications and the potential impact of such control on sovereignty and self-determination where they are largely foreign-owned, the above-mentioned Task Force recommended that special requirements as to ownership and control by nationals be imposed on computer-based information services, offered on a regular basis to the public at large and conveying cultural values analogous to those conveyed by broadcasting systems". 83/

Television and radio broadcasting

76. Proposed measures to deal with problems arising from television broadcasting via communications satellites are at present under discussion in the United Nations family. References to approaches suggested or taken may be found in the Secretary-General's report on respect for the privacy of individuals and the integrity and sovereignty of nations in the light of advances in recording and other techniques. 84/

77. Legislative and other action has been taken in a number of countries to ban subliminal messages in broadcasting.

82/ United States, Communications Act of 1934, as amended (47 USC section 202 (a)) cited in S. B. Perlman, Legal Aspects of Selected Issues in Telecommunications (Montvale, N.J., AFIPS Press, 1976). p. 4.

83/ Branching Out, vol. I, p. 206, recommendation 25.

84/ See E/CN.4/1116/Add.3 and Corr.1, paras. 34 to 76. See also provisional agenda of the twenty-ninth regular session of the General Assembly (A/9700), item 33 (International co-operation in the peaceful uses of outer space: report of the Committee on the Peaceful Uses of Outer Space) and item 34 (Preparation of an international convention on principles governing the use by States of artificial earth satellites for direct television broadcasting: report of the Committee on the Peaceful Uses of Outer Space).

78. Subliminal messages of any kind (and not only subliminal advertising) were banned in the United Kingdom by the Television Act, 1964 (section 3 (III)). Under the provisions of that Act, the Independent Television Authority of the United Kingdom is to satisfy itself that the programmes broadcast by the Authority do not include any technical device which, by using images of very brief duration or by any other means, exploits the possibility of conveying a message to, or otherwise influencing the minds of, members of the audience without their being aware, or fully aware, of what has been done. The British Broadcasting Corporation (B.B.C.) is also prohibited from using this type of television broadcast. The Institute of Practitioners in Advertising, the trade association of advertising agencies in the United Kingdom, has condemned subliminal advertising and the use of hypnosis as advertising techniques. 85/

79. In the United States, the television code of the National Association of Broadcasters includes a provision which reads:

> "Any technique whereby an attempt is made to convey information to the viewer by transmitting messages below the threshold of normal awareness is not permitted."

80. The application of the code is supervised by the Association's Television Code Authority. 86/

81. In Belgium, draft legislation on the protection of privacy, introduced in 1972, contained a provision which would make the projection of subliminal messages an offence punishable by imprisonment for from one to five years and a fine of from 1,000 to 100,000 Belgian francs. The penalty would apply to anyone who by any means whatever projects images or sensations which, though not consciously perceived, are capable of influencing behaviour. 87/

82. "Subliminal advertising and propaganda" were included by the Consultative Assembly of the Council of Europe among the newly developed techniques which it believed to be a threat to the rights and freedoms of individuals and which led the Consultative Assembly to recommend in 1968 that a study be undertaken concerning the adequacy of legislation in States members of the Council to protect the right to privacy against violations which may be committed by the use of modern scientific and technical methods. 88/

85/ Information forwarded by the Government of the United Kingdom on 17 December 1969.

86/ The New York Times, 27 December 1973.

87/ Draft law dated 26 January 1972, forwarded by the Government of Belgium on 15 February 1973.

88/ Consultative Assembly of the Council of Europe, Recommendation 509 (1968) on human rights and modern scientific and technological developments.

83. The Ligue Internationale contre la concurrence déloyale in 1969 rejected the use of subliminal advertising on the grounds that it constituted a violation of the dignity and of the freedom of thought of the individual. 89/

2. Question of draft international standards concerning the uses of electronics which may affect the rights of the person

84. In view of the fragmentary nature of the information available so far on effective safeguards and remedies, it would be premature to offer points relating specifically to computer communications for possible inclusion in draft international standards in the three areas discussed, with the possible exception of suggesting that provisions be adopted which would prohibit the use of subliminal messages in broadcasting and make such use subject to penal sanctions under national law. In view of the increasing importance of these uses of electronics it may, however, be appropriate to attempt to elaborate such points when further experience has been gained in observing the impact on human rights of electronic communications techniques.

85. A start might, however, be made in considering the possibility of drawing up international standards to ensure generally the integrity of information stored on electronic data processing media. These standards might provide, for example, for such measures as magnetic coding of tapes and other storage media with a view to protecting access to the information stored and safeguarding it from unauthorized alteration; and for setting up procedures for what is technically referred to as an "audit trail", which leaves a record of every access to and change made in the information stored. 90/

86. Standards concerning television broadcasts via communication satellites are under discussion by other organs of the United Nations. 91/

89/ K. Greifelt, rapporteur, new item 5, "Subliminal advertising", Ligue Internationale contre la concurrence déloyale, Congress held at Vienna, Austria, 25-29 May 1969; also Commentary on article 8 (1) accompanying Belgian draft law of 26 January 1972 (see foot-note 67, above).

90/ Cf. physical security measures and technological safeguards discussed in document E/CN.4/1142, paragraphs 125 to 165; while some of the measures mentioned in these paragraphs are meant more specifically to protect personal data, many of them are applicable to the storage of any information whatever. Reference to "audit trail" procedures may be found in paragraph 155 of document E/CN.4/1142.

91/ Cf. items 33 and 34 of the provisional agenda of the twenty-ninth session of the General Assembly (A/9700). See foot-note 84, above.

APPENDIXES

Appendix A

THE LIBRARY OF CONGRESS

Congressional Research Service

WASHINGTON, D.C. 20540

July 14, 1976

TO : Senate Constitutional Rights Subcommittee
Attention: Douglas Lea

FROM : American Law Division

SUBJECT: Privacy Bills Introduced in the 94th Congress: Index and Digests

This will refer to your request for an up-to-date compilation of digests of privacy-related bills introduced in the 94th Congress. We are enclosing a compilation prepared through a search of our computerized Bill Digest index files. In addition to the digests, this compilation contains the names of all sponsors and co-sponsors for each bill, the date of introduction, the Committee to which the bill was referred, and action, if any, taken on each bill.

Since this compilation is to be used as part of a compendium of papers on surveillance technology, we have emphasized bills related to surveillance and national security. The following index terms were used to conduct our search: right of privacy, eavesdropping, wiretapping, confidential communications, electronic surveillance, privacy, surveillance, surveillance activities, criminal records, bank records, medical records, telephone privacy act, intelligence agencies and polygraphs.

We have also provided a subject index to the compilation, which is enclosed.

E. Jeremy Hutton
Legislative Attorney

THE LIBRARY OF CONGRESS

Congressional Research Service

WASHINGTON, D.C. 20540

SUBJECT INDEX TO BILLS INTRODUCED IN
94TH CONGRESS RELATING TO PRIVACY (THRU 7/6/76)

Bank Records: see Financial Privacy Act.

Bill of Rights Procedures Act: S. 1888, 3349; H.R. 214, 414, 2330, 2603, 2604, 3113, 3467, 3855, 3874, 10425, 14284.

Census, to authorize limited disclosure of records: H.R. 11337.

Census, to eliminate penalties for refusal to answer: H.R. 3754, 77856.

Census, to increase penalties for unauthorized disclosure: H.R. 11337.

Census, to protect privacy and limit information sought: S. 775; H.R. 2556, 7824, 8007.

Classified Materials, Unauthorized disclosure: H.R. 13602.

Common Carrier Employees, to limit surveillance by: S. 3349; H.R. 10425; see Bill of Rights Procedures Act.

Central Intelligence Agency, to prohibit domestic surveillance: S. 244.

Central Intelligence Agency, to remove Privacy Act exemptions: H.R. 169, 2635, 5128, 5129.

Congress, to permit receipt of personal information from agencies; Privacy Act exemption: H.R. 9920, 9925, 9942, 9951, 10136, 10159, 10368.

Credit cards, to limit transfer of information pertaining to holder: S. 3057, 3559.

Credit Reporting Act, amend: H.R. 1324, 8661, 8802.

Criminal records or criminal justice information: S. 1427, 1428, 2008; H.R. 61, 338, 662, 8227, 8661, 8802.

Domestic Security Guideline, disapproval: H. Res. 1037.

Financial Privacy Act: S. 1343, 3349; H.R. 214, 550, 1005, 2752, 7482, 7483, 7649, 8306, 8806, 10425, 13757.

Foundations, private, protect privacy of some recipients: H.R. 2713.

Government employees and applicants, to protect privacy of: S. 1887; H.R. 564, 720, 1173, 1174, 1910, 2596, 5437, 5438, 9002.

Government records: see Personal information records, to protect privacy of and provide means for correction by Government record subjects; and specific agencies.

Intelligence agencies, to permit G.A.O. audits of expenditures: S. 653.

Internal Revenue Service, audit disclosure and procedures: S. 136, 442, 2342; H.R. 615, 5819, 5820, 9599, 9735, 9822, 10387 10960, 11090.

Internal Revenue Service, limit dissemination and disclosure of tax information: S. 199, 1511, 2324, 2380, 3405; H.R. 616, 955, 1779, 3732, 4193, 4194, 4195, 4433, 5198, 5410, 5469, 5569, 6013, 6390, 6712, 6713, 6714, 9599, 9735, 9322, 10960, 11090, 11307, 11780, 11953.

Internal Revenue Service, limit dissemination to states: H.R. 11953.

Investigative consumer report, to regulate: H.R. 1324.

Mail covers, to Limit: S. 1888, 3349; H.R. 214, 414, 2330, 2603 2603, 2604, 3113, 3467, 3855, 3874, 10425, 14284; see Bill of Rights Procedures Act.

Mailing lists: H.R. 1464.

Marital prefixes, to prevent unnecessary requests: H.R. 8248.

Medical records: H.R. 2885, 5515, 11105, 11511, 11896, 12624.

Military surveillance of civilians, to prohibit: S. 84; H.R. 142, 266, 539, 1185, 2455, 2753, 2754, 2862, 3113, 3284, 4339, 7856.

National Commission for review of federal and state wiretap laws: S. 2757, H.R. 11129.

National Security Surveillance Act: S. 743.

Newsmen's Right to Privacy Act: H.R. 215, 562, 3655.

Personal information records, to protect privacy of all record system subjects: H.R. 1984, 3235, 3236, 3237, 7234.

Personal information records, to protect privacy of and provide means for correction by government record subjects: H.R. 169, 1098, 2635, 5128, 5129.

Polygraph tests, to restrict use: S. 1841; H.R. 564, 2596, 5437, 5438, 9002, 13191.

Privacy Board, to establish: H.R. 1984, 3235, 3236, 3237, 7234.

Privacy Protection Study Commission, authorization: S. 3435; H.R. 13681, 13682.

Right to privacy, comprehensive act: H.R. 1984, 3235, 3236, 3237, 7234.

School employee records: H.R. 623.

School records, to limit federal access: H.R. 2213, 2819.

Surveillance, to authorize warrant for foreign intelligence: S. 743, 3197; H.R. 12750, 13120. 13197, 13376, 13605.

Surveillance, to establish congressional committee on: S. 189.

Surveillance Practice and Procedures Act: H.R. 141, 9515.

Surveillance, to restrict civil: H.R. 1864, 2566, 7856. See also: Military surveillance; Bill of Rights Procedures Act.

Tax: See Internal Revenue Service.

Telephone Privacy Act: S. 1612; H.R. 2572, 9165, 9666.

Veterans' Administration, permit release of records: H.R. 5324.

Wiretapping and electronic surveillance: S. 743, 1888, 3197; H.R. 141, 171, 214, 414, 620, 1603, 2330, 2453, 2603, 2604, 3467, 3855, 3874, 9515, 12750, 13120; See also Bill of Rights Procedures Act.

E. Jeremy Hutton

E. Jeremy Hutton
Legislative Attorney
American Law Division
July 13, 1976

PRIVACY BILLS - 94th CONGRESS - CRS DATA BASE - 07/06/76

SENATE BILLS

S. 84. Mr. Mathias; 1/15/75. Judiciary.
Cosp: Bayh, Cranston, Hart (Mich.), Hartke, Haskell, Javits, Leahy, McGovern, Tunney, Williams.

Freedom from Military Surveillance Act - Restricts the actions of any civil officer of the United States or any member of the Armed Forces of the United States in using the Armed Forces of the United States to exercise surveillance of civilians or to execute the civil laws.

Sets forth penalties for violations of the provisions of this Act.

S. 136. Mr. Montoya; 1/15/75. Finance, Church, Goldwater, Hatfield, Javits, Laxalt, Mathias, Tunney.

Taxpayer Audit Disclosure Act - Requires the establishment of formal procedures and criteria for the selection of individual income tax returns for audit. Directs the Secretary of the Treasury or his delegate to provide any individual selected for auditing with a written notice which clearly specifies the reasons for and the manner in which the return of such individual was selected for audit

Provides that the Secretary or his delegate shall furnish to such individual a written explanation which describes the audit procedure, the rights which a taxpayer may exercise during such procedure, the right of the taxpayer to make an administrative or judicial appeal from an adverse decision at the end of such procedure, and the right of the taxpayer to claim a refund.

Requires the Secretary of the Treasury or his delegate to submit to the Joint Committee on Internal Revenue Taxation, before September 30 of each year, a report setting forth: (1) the number of individuals whose returns were selected for audit during the previous 12-month period; (2) a classification of individuals whose returns were audited during the previous 12-month period by, among other factors, income levels, geographic distribution, and profession; (3) the number of individuals audited during the previous 12-month period who were found to have made underpayments or overpayments of tax, together with summary statistics reflecting the percentage of such number, by income category, who made underpayments or overpayments of certain ranges of amounts (to be determined by the Secretary or his delegate); and (4) such other information as may be requested by the joint committee in accordance with the purposes of this Act.

S. 189. Mr. Nelson; 1/16/75 Government Operations, Jackson Muskie

Establishes in the Congress a Joint Committee on the Continuing Study of the Need to Reorganize the Departments

and Agencies Engaging in Surveillance.

Sets forth the membership of the Committee.

States that it shall be the function of the joint committee: (1) to make a continuing study of the need to reorganize the departments and agencies of the United States engaged in the investigation or surveillance of individuals, (2) to make a continuing study of the intergovermental relationship between the United States and the States insofar as that relationship involves the area of investigation or surveillance of individuals; and (3) to file reports at least annually, and at such other times as the joint committee deems appropriate, with the Senate and the House of Representatives, containing its findings and recommendations with respect to the matters under study by the joint committee.

Requires that the joint committee shall, at least annually, receive the testimony under oath, of a representative of every department, agency, instrumentality, or other entity of the Federal Government, which engages in investigations or surveillance of individuals. States that such testimony shall relate to: (1) the full scope and nature of the respective department's agency's instrumentality's, or other entity's investigations or surveillance of individuals; and (2) the criteria, standards, guidelines, or other general basis utilized by each such department, agency, instrumentality, or other entity in determining whether or not investigative or surveillance activities should be initiated, carried out, or maintained.

Sets forth the powers of the Committee.

Specifies that the provisions of this Act shall not in any way limit or otherwise interfere with the jurisdiction or powers of any committee of the Senate, or the House of Representatives, or of Congress to request or require testimony or the submission of information from any representative of any department, agency, instrumentality, or other entity of the Federal Government.

S. 199. Mr. Weicker; 1/17/75. Finance, Abourezk, Allen, Baker, Beall, Brooke, Buckley, Cannon, Case, Church Clark, Cranston, Dole, Domenici, Eagleton, Goldwater, Gravel, Hansen, Hart (Mich.), Hartke, Hathaway, Humphrey, Javits, Kennedy, Laxalt, Leahy, Mathias, McGee, McGovern, Metcalf, Mondale, Montoya Percy, Stafford, Symington, Taft, Tunney, Williams.

States that all tax returns made with respect to taxes imposed by the Internal Revenue Code are confidential records, and that, except where provided otherwise, no return shall be open to inspection nor shall information contained therein be disclosed.

Authorizes inspections of returns by the following persons: (1) the taxpayer or his representative; (2)

officers and employees of the Departments of Justice, the Treasury, State agencies entrusted with carrying out the income tax laws, and the Internal Revenue Service solely for administration and enforcement of the income tax laws; and (3) the President of the United States.

Authorizes the disclosure of statistical information to State and Federal agencies and the Joint Committee on Internal Revenue

Imposes civil and criminal penalties for violations of this Act

S. 244. Mr. Proxmire; 1/17/75. Armed Services, Cranston, Kennedy, Pell.

Revises the National Security Act to prohibit domestic intelligence activities by the Central Intelligence Agency, directly or indirectly or in cooperation with other agencies. Prohibits the Central Intelligence Agency from participating in any illegal activity within the United States.

S. 442. Mr. Bentsen; 1/28/75. Finance.

Provides that whoever initiates or conducts, or attempts to initiate or conduct, an income tax audit, investigation, or prosecution for reasons other than enforcement of the Internal Revenue Code or on account of race creed, color, or political status shall be fined not more than $10,000 or imprisoned for not more than 5 years or both.

Directs the Comptroller General to report annually to the committees of the Congress charged with the promulgation of the Federal tax laws on the effectiveness and impartiality of the administation of such laws. Specifies the powers and duties of the Comptroller General with respect to the conduct of investigations of the administration of the Federal tax laws.

Increases the criminal penalties for unauthorized disclosure of confidential tax information to a fine of up to $5000 or 5 years' imprisonment or both. Makes any person disclosing such information without authorization personally liable to any taxpayer injured by such disclosure up to $20,000 actual and punitive damages.

Authorizes inspections of income tax returns by officers and employees of the Internal Revenue Service, Department of the Treasury, the Department of Justice, and State agencies charged with the administration of State tax law, in each case solely for purpose of administration and enforcement of the tax laws

Specifies procedures for the disclosure of income tax return information to committees of Congress.

Provides that a person, partner in a partnership, or a corporation with respect to whom the return is filed shall, upon written request, have an opportunity to inspect such return.

Authorizes the Commissioner of Internal Revenue to disclose return information to correct misstatements of

published or disclosed facts.

S. 653. Mr. Proxmire; 2/7/75. Government Operations.

Permits audits by the General Accounting Office of expenditures by intelligence agencies upon request of any committee of the Congress which has legislative jurisdiction over such agency or the appropriation of funds therefor.

Lists the agencies included within the term "intelligence agency".

Provides for the submission of a report of any such audit requested to the committee making such request.

S. 743. Mr. Nelson; 2/19/75. Judiciary, Kennedy.

National Security Surveillance Act - States the finding of the Congress that no adequate controls exist to govern the conduct of electronic surveillance on grounds of national security. Makes it the purpose of this Act to establish administrative practices, procedures, and standards under which prior court authorization must be obtained for any electronic surveillance conducted on grounds of national security or on any other ground.

Provides that a communication common carrier shall not install any device to intercept a wire or oral communication, or otherwise allow its resources to be used to assist in the interception of a wire or oral communication, unless the Government officer requesting such installation or assistance provides a copy of a court order authorizing the interception. Provides that no communication common carrier shall assist any interception beyond the date authorized in the court order, except upon receipt of a court order extending the time period.

Provides that the Attorney General, or any Assistant Attorney General specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or any Federal department, agency, or other unit having lawful responsibility for the investigation of the offense as to which application is made, when: (1) there is probable cause to believe that the target has committed or is about to commit an offense punishable by death or by imprisonment for more than one year under specified provisions of Federal law related to the enforcement of the Atomic Energy Act of 1954, or to espionage, sabotage, or treason; and (2) such interception will probably provide evidence concerning the commission of that offense.

Provides for procedures for wire and oral communications interception relating to military security and national defense.

Requires that in January, April, July, and October of each year, the Attorney General shall report to the Committee on the Judiciary and on Foreign Relations of the Senate and the Committees on the Judiciary and on Foreign

Affairs of the House of Representatives specified information with respect to interceptions of wire or oral communications made during the preceding three months.

S. 775. Mr. Chiles; 2/20/75. Post Office and Civil Service, Baker, Laxalt, McGovern.

Stipulates that in conducting the decennial census the Secretary of Commerce shall require information to be furnished only with respect to the following items: (1) name and address; (2) relationship to head of household; (3) sex; (4) date of birth; (5) race or color; and (6) visitors in the home at the time of the census. [Adds 13 U.S.C. 141 (c)]

Provides that refusal or neglect to furnish information not within such categories shall not be an offense. [Amends (3 U.S.C. 22 (a)]

S. 1343. Mr Cranston; 3/26/75.
Banking, Housing and Urban Affairs, Brock, Church, Gravel, Hart (Mich.), Haskell, Huddleston, Humphrey, Johnston, Laxalt, Mathias, McGovern, Montoya, Muskie, Percy, Scott (Pa.), Taft, Thurmond, Tunney, Weicker.

Right to Financial Privacy Act - States that the purposes of this Act are to protect and preserve the confidential relationship between financial institutions and their customers and the constitutional rights of those customers, and promote commerce by prescribing policies and procedures to insure that customers have the same right to protection against unwarranted disclosure of customer records as if the records were in their possession.

Prohibits any Federal agency or employee, or any State or local government from obtaining copies of, access to, or the information contained in, the financial records of any customer from a financial institution unless the financial records are described with particularity and: (1) such customer has authorized such disclosure in accordance with this Act; (2) such financial records are disclosed in response to an administrative subpena or summons; (3) such financial records are disclosed in response to a court order; or (4) such financial records are disclosed in response to a judicial subpena.

States that no financial institution may provide a Federal agency or employee, or any State or local government, copies of or the information contained in the financial records of any customer except in accordance with the requirements of this Act.

Sets forth provisions governing customer authorization, administrative subpenas and summons and judicial subpenas.

Provides that the Secretary of the Treasury may not require an institution to maintain any financial records or to transmit any reports relating to customers unless: (1) such records are required for use by a supervisory agency in the supervision of that institution; or (2) such records are

required to be maintained by the Internal Revenue Code.

Prescribes civil and criminal penalties for violation of the provisions of this Act.

S. 1427. Mr. Tunney; 4/14/75. Judiciary.

Criminal Justice Information Control and Protection of Privacy Act - Title I: Findings and Declaration of Policy; Definitions; Applicability - Declares that in order to insure the security of criminal justice information systems, and to protect the privacy of individuals named in such systems, it is necessary and proper for the Congress to regulate the exchange of such information. Sets forth the definitions of terms used in this Act. Describes the information systems to which this Act applies, including those operated by the Federal Government, and to which it does not apply, including original books of entry or police blotters.

Title II: Collection and Dissemination of Criminal Justice Information, Criminal Justice Investigations Information and Criminal Justice Intelligence Information - Prescribes the procedure for: (1) dissemination, access, and use of criminal justice information by criminal justice agencies; (2) dissemination of identification record and wanted persons record information; (3) dissemination, access, and use of criminal justice information by noncriminal justice agencies; and (4) dissemination, access, and use of criminal justice information with respect to appointments and employment investigations.

Prohibits agencies having access to criminal justice information from disseminating it to others not authorized to have it or from using it for a purpose not authorized by this Act, with limited exceptions with regard to rehabilitation officials.

Places limitations on access to criminal justice information via categories other than name.

Requires every agency information system covered by this Act to promulgate regulations on security, accuracy, updating and purging. Sets out what such regulations must provide. Requires every agency or information system to establish a process for access and challenge of incorrect or inacurrate information. Details what such regulations must provide.

Places limitations on the collection and dissemination of intelligence information. States that such information may not be maintained in automated systems and must be kept separate and apart from all other criminal justice files.

Enumerates the conditions under which criminal justice investigative information may be disclosed.

Title III: Administrative Provisions; Regulations; Civil Remedies; Criminal Penalties - Creates a Criminal Justice Information Systems Board to have responsibility for the administration and enforcement of this Act.

Requires each State to establish a central administrative agency, separate and apart from existing criminal justice agencies, with authority to oversee

operation of criminal justice information systems in that State.

Requires every information system or agency to give public notice, once annually, of the type of information it collects and disseminates, its sources, purpose, administrative director and other pertinent information.

Requires audits of systems and agencies which collect and disseminate information. States that such audits are to be conducted by the Board, by the State agency, and by each criminal justice system.

Permits the Federal Government to operate an interstate criminal justice information system under the policy control of the Board. Limits information contained in such system.

Lists administrative actions that may be taken by the Board in the event that a criminal justice information system is found to have violated any provision of this Act.

Provides the judicial machinery for the exercise of the right granted in this Act. Provides that aggrieved individuals may obtain both injunctive relief and damages, $100 recovery for each violation, actual and general damages, and attorney's fees.

Provides criminal penalties for violations of this Act.

Provides that any State regulation which imposes stricter privacy requirements on the operation of criminal justice information systems or upon the exchange of criminal justice information takes precedence over this Act or any regulations issued pursuant to this Act.

Authorizes the appropriation of such funds as the Congress deems necessary for the purposes of this Act.

S. 1428. Mr. Tunney; 4/14/75. Judiciary.

Criminal Justice Information Control and Protection of Privacy Act - Title I: Purpose and Scope - Expresses the findings of Congress and the basis for this Act. Defines the terms used in this Act and the criminal justice agencies to which this Act applies, including agencies which exchange information interstate. Specifies the records and proceedings to which this Act does not apply, including court records of public criminal proceedings.

Title II: Collection, Dissemination, and Use of Criminal Justice Information - Requires criminal justice agencies to publish regulations specifying the type of information systems maintain, the limits on use of such information, and additional enumerated regulations. Requires the adoption of specified protective internal operating procedures by such agencies. Places the same limitations on data obtained from a foreign government.

States that identification information may be disseminated for official purposes but when such information includes arrest record or ciminal record information, dissemination shall be only as permitted by this Act.

Prescribes procedures governing: (1) access to automated criminal justice information systems, which shall be by formal written agreements; (2) dissemination, access, and use by noncriminal justice agencies; (3) access for

appointments and employment investigations; and (4) secondary use of criminal justice information.

Requires each agency to adopt procedures to insure physical security, continued accuracy, corrections and information, and periodic reviews.

Outlines the procedures for access by individuals for purpose of challenges.

States that criminal justice intelligence and investigative information may be collected by a criminal justice agency only for official purposes. Enumerates the internal operating procedures to be adopted by such agencies.

Title III: Administration and Enforcement - Establishes in the executive branch the Commission on Criminal Justice Information, describing its powers and duties, including to appraise the laws, policies and practices of Federal, State, and local governments with respect to criminal justice information systems.

Requires each agency to adopt procedures relating to administrative sanctions.

Provides judicial remedies to individuals denied access to information concerning themselves in violation of this Act. Declares that any State or local agency participating in a criminal justice information system subject to this Act shall be deemed to have consented to the bringing of actions under this Act.

Authorizes to be appropriated funds necessary to carry out the provisions of this Act.

S. 1472. Mr. Dole; 4/18/75. Finance.

Provides, under the Social Security Act, for the establishment and revision of Professional Standards Review Organization areas, such establishment and revision to take into account the recommendations of the doctors of medicine or osteopathy.

States that the final determination in the establishment or revision of any Professional Standards Review Organization area shall be subject to review in a civil action commenced by any interested person.

Directs the National Professional Standards Review Council to conduct a study for the purpose of evaluating whether, and under what conditions, organizations other than professional associations shall be allowed to perform review functions.

Requires each Professional Standards Review Organization to assume responsibility for professional standards review of health care services furnished by or in institutions operated by the Public Health Service and the Veterans Administration in the area which it serves.

Requires, in conjunction with such reviews, that procedures be developed whereby deficiencies shall be brought to the attention of administrators of the hospitals and other Federal institutions concerned. Calls for the consolidation of data and reports compiled under these provisions.

Directs that criteria of health care shall be identified or developed by each Professional Standards Review Organization, giving due consideration to such criteria of care identified or developed by national medical specialty organizations. States that such criteria of care shall be used by the Professional Standards Review Organization as guides of care.

Requires the National Professional Standards Review Council to provide for the distribution to each Professional Standards Review Organization, and to each other agency performing review functions, of appropriate materials indicating various guides being utilized in other geographical areas.

Provides for the protection of the confidentiality of medical records compiled under this Act.

Empowers the Secretary of Health, Education, and Welfare to enter into a contract with any State medical society or private nonprofit organization (including medical foundations) designated by a State medical society for the provision of necessary technical and other assistance in the creation and operation of local professional standards review organizations.

S. 1511. Mr. Montoya; 4/23/75. Finance.

Tax Return Privacy Act - Provides that tax returns shall be considered confidential, as opposed to public, records under the Internal Revenue Code.

Requires, as a general rule, written consent by the taxpayer before the Government may inspect such taxpayer's returns. States that this rule shall not apply to (1) State income tax inspections by the appropriate State agency; (2) inspection of a corporate return by a shareholder; (3) inspection by Congressional committees with jurisdiction over taxation; and (4) inspections by Justice or Treasury Department officials for administration or enforcement purposes.

Authorizes Federal district courts to grant an order authorizing an inspection of a tax return upon a showing of probable cause to believe that the return contains information necessary to a prosecution or investigation.

Allows the President to authorize the release of tax information concerning a prospective appointee to Federal office.

Increases the criminal penalties for the unauthorized disclosure of information under the Internal Revenue Code.

S. 1612. Mr. Nelson; 5/1/75. Judiciary, Tunney.

Communications Privacy Act - Prohibits, under the Communications Act of 1934, all disclosures of telephone records except through service of a court subpena meeting specified criteria

Requires in all cases except where the telephone subscriber is a foreign power, that the party subpenaing the records notify the subscriber simultaneously that records of

his telepone conversations are being subpenaed. Allows such notification to be postponed if the Government satisfies the court that notification would impede an ongoing criminal investigation or would hamper the Government's ability to protect national security interests.

Prohibits the telephone company from responding to such a subpena for at least ten days.

S. 1841. Mr. Bayh; 6/2/75. Judiciary, Abourezk, Mathias, Tunney.

Makes it unlawful for any Government employee or officer or any person engaged in business or other activity affecting interstate commerce to: (1) require a polygraph test as a condition of employment; or (2) discharge or deny a promotion to an individual who refuses to submit to a polygraph test.

Permits civil suits to enforce the provisions of this Act. Gives the U.S. district courts jurisdiction under this Act without regard to amount of pecuniary injury or exhaustion of administrative remedies.

S. 1887. Mr. Tunney; 6/5/75. Judiciary, Abourezk, Bayh, Burdick, Fong, Mathias, Scott (Pa.), Thurmond.

Makes it unlawful for any Executive Branch officer or any person acting under such officer's authority to require that any United States Government employee or any applicant for employment in the Executive Branch of the Government do any of the following: (1) disclose their race, religion, or national origin; (2) attend Government-sponsored meetings and lectures or participate in outside activities unrelated to their employment; (3) report on their outside activities or undertakings unrelated to their work; (4) submit to questioning about their religion, personal relationships or sexual attitudes through interviews, psychological tests, or polygraphs; or (5) support political candidates or attend political meetings.

Permits inquiries into national origin when necessary for the national interest or overseas work. Allows agency officers to advise employees of charges of sexual misconduct as long as the employee has an opportunity to refute the charge.

Makes it illegal to coerce an employee to buy bonds or make charitable contributions; or to require him to disclose his own personal assets, liabilities, or expenditures, or those of any member of his family unless they would show a conflict of interest.

Provides a right to have a counsel or other person present, if the employee wishes, at an interview which may lead to disciplinary proceedings.

Makes it unlawful for any Civil Service Commission officer to require any executive department or agency to do any prohibited act; or to require a person seeking to establish Civil Service status or employment in the executive branch to submit to interrogation, polygraph

testing, or psychological testing designed to elicit views regarding religion, personal relationships, or sexual attitude.

Accords the right to a civil action in a Federal court for violation or threatened violation of this Act.

Directs the Attorney General to defend all persons sued who acted pursuant to an order or who, in his opinion, did not willfully violate this Act.

Establishes a three-member Board on Employees' Rights with members appointed by the President by and with the advice and consent of the Senate. Grants the Board the authority and duty to receive and investigate written complaints from any person claiming to be aggrieved by any violation or threatened violation of this Act and to conduct a hearing on each such complaint. Grants the Board powers which will eliminate violation of this Act. Directs the Board to make an annual report of its activities to Congress.

Excludes the Central Intelligence Agency and the National Security Agency from the provisions of this Act.

Permits the establishment of agency grievance procedures to enforce this Act, but the existence of such procedures shall not preclude the use of other remedies.

S. 1888. Mr. Mathias; 6/5/75. Judiciary, Hart (Mich.), Hatfield, Javits, Kennedy, Mansfield, Nelson, Pearson.

Bill of Rights Procedures Act - States that it is the purpose of this Act to prohibit any interception of communication, other electronic surveillance, surreptitious entry, mail opening, or the inspection of and procuring of the records of telephone, bank, credit, medical, or other business or private transactions, of any individual without a court order issued upon probable cause that a crime has been or is about to be committed, supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.

Provides that whoever, being an officer, agent, or employee of the united States or any department or agency thereof, willfully: (1) searches any private dwelling used and occupied as a dwelling without a warrant directing such search or malicously and without reasonable cause searches any other building or property without a search warrant; (2) procures or inspects the records of telephone calls, bank, credit, medical, or other business or private transactions of any individual without a search warrant or the consent of the individual; (3) opens any foreign or domestic mail not directed to him without a search warrant directing such opening or without the consent of the sender or addressee of such mail; or (4) intercepts, endeavors to intercept, or procures any other person to intercept any wire or oral communication except as authorized by law; shall be fined not more than $10,000 or imprisoned not more than one year, or both.

Requires that within 30 days after the date of an order

authorizing or approving the intereception of a wire or oral communication (or each extension thereof) entered under authority of law, or the denial of an order approving an interecption, the person seeking such order shall report to the Administrative Office of the United States Courts and to the Committees on the Judiciary of the Senate and House of Representatives: (1) the fact that an order or extension was applied for; (2) the kind of order or extension applied for; (3) the fact that the order or extension was granted as applied for, was modified, or was denied; (4) the period of interceptions authorized by the order, and the number and duration of any extensions of the order; (5) the names of all parties to the intercepted communications; (6) the offense specified in the order or application; (7) the identity of the investigative or law enforcement officer and agency making the application and the person authorizing the application to be made; (8) a copy of the court order authorizing, approving, or denying such interception; and (9) the nature of the facilities from which or the place where communications were intercepted.

Specifies that reports be made within 90 days after the date of an order approving the interception of a wire or oral communication on the disposition of all records of any such interception and the identity of and action taken by all individual who had access to any such interception.

Sets forth reporting requirements in the case of warrants issued authorizing the opening of mail.

S. 2008. Mr. Tunney; 6/25/75. Judiciary.

Criminal Justice Information Control and Protection of Privacy Act - Title I: Purposes and Scope - Declares it to be the finding of Congress that effective law enforcement requires the dissemination of complete and accurate criminal justice information; but the irresponsible use of inaccurate information may infringe on individual rights. Defines terms used in this Act. Lists the criminal justice agencies to which this Act applies, including: (1) agencies which exchange information interstate; and (2) information obtained from a foreign government or international agency to the extent it is comingled with information obtained from domestic sources. Lists the records and proceedings to which this Act does not apply, including original books of entry or police blotters, and court records of public criminal proceedings.

Title II: Collection and Dissemination of Criminal Justice Information; Criminal Justice Investigative Information; and Criminal Justice Intelligence Information - Prescribes the procedures for: (1) dissemination, access, and use of criminal justice information by criminal justice agencies; (2) dissemination of identification record and wanted persons record information; (3) dissemination, access, and use of criminal justice information by noncriminal justice agencies; and (4) dissemination, access, and use of criminal justice information with respect to appointments and employment investigations.

Prohibits agencies having access to criminal justice information from disseminating it to others not authorized to have it or from using it for a purpose not authorized by this Act, with limited exceptions with regard to correctional officials.

Requires requests for information to identify the individual to whom the information relates by name except when the information is requested in connection with research related to the administration of criminal justice or in developing investigative leads for a particular offense.

Directs each criminal justice agency to adopt procedures providing: (1) for the security, accuracy, and updating of criminal justice information; and (2) for the sealing and purging of criminal justice information. Provides for access to criminal justice information by an individual or his attorney for purposes of challenging the accuracy, completeness, legality of such information. Requires criminal justice agencies to adopt rules to implement the granting of such access.

Places limitations on the collection and dissemination of intelligence information. Prohibits direct remote terminal access to criminal justice information except for specified types of information. Enumerates the conditions under which criminal justice investigative information may be disclosed.

Title III: Administrative Provisions; Regulations; Civil Remedies; Criminal Penalties - Establishes the Commission on Criminal Justice Information. States that the Commission shall have overall responsibility for the administration and enforcement of this Act. States that the Commission shall be composed of 13 members, including the Attorney General and nine members appointed by the President with the advice and consent of the Senate. Sets five years as the duration of the Commission.

Sets forth the powers and duties of the Commission, including the issuance of such regulations, interpretations and procedures as are necessary to effectuate the provisions of this Act. Authorizes the Commission to conduct hearings, and to exercise subpena powers to insure the presence of witnesses or evidence. Directs the Commission to encourage the formation of State agencies to carry out the provisions of this Act.

Provides judicial remedies to persons aggrieved by a violation of this Act or regulations issued pursuant to this Act. Provides for both injunctive relief and damages of not less than $100 per violation and reasonable attorneys' fees and costs. Directs that any Government employee who willfully violates this Act shall be fined not more than $10,000.

Authorizes the appropriation of such funds as the Congress deems necessary for the purposes of this Act.

S. 2324. Mr. Dole; 9/10/75. Finance.

Income Tax Return Confidentiality Act - States that a

tax return filed with respect to taxes imposed under the Internal Revenue Code shall be open to inspection solely by the taxpayer who files such return, except that inspection may be had: (1) by officers and employees of the Department of the Treasury whose official duties with respect to Federal tax administration require such inspection; (2) by attorneys of the Department of Justice, including United States Attorneys, upon written request, solely for use in connection with an investigation conducted by such attorneys or in preparation by such attorneys for a proceeding before a Federal grand jury or a Federal or State court only under specified conditions if the taxpayer whose return of tax is to be inspected consents; (3) by Federal and State agencies regulating tax return preparers; (4) by employees of the United States in the course of a criminal investigation and pursuant to a search warrant; (5) by the Social Security Administration, Railroad Retirement Board, Department of Labor, and Department of Health, Education, and Welfare in appropriate cases; (6) for statistical studies by the Social and Economic Statistics Administration; (7) for investigation of Federal appointees; (8) by committees of Congress with tax law jurisdiction; (9) for State tax administration purposes; (10) for judicial and administrative proceedings related to tax administration; and (11) by an agent of a partnership or corporation who has a substantial interest in such return.

Requires the Secretary of the Treasury to report annually to the Joint Committee on Internal Revenue Taxation on all requests received under this Act to inspect a return of tax or for disclosure of information derived from a return of tax and the disposition of such requests.

S. 2342. Mr. Magnuson; 9/16/75. , Case, Church, Goldwater, Hart (Mich.), Haskell, Hatfield, Hathaway, Humphrey, Inouye, Jackson, Javits, Kennedy, Mansfield, McGovern, McIntyre, Mondale, Montoya, Proxmire, Ribicoff, Roth, Tunney.

Federal Taxpayers' Rights Act - Directs the Secretary of the Treasury to prepare pamphlets which set forth in nontechnical terms: (1) the rights and obligations of a taxpayer and the Service during an audit; (2) the procedures by which a taxpayer may appeal any adverse decision of the Service (including administrative and judicial appeals); (3) the procedures for prosecuting refund claims and filing of taxpayer complaints; and (4) the procedures which the Service may use in enforcing the internal revenue laws (including assessment, jeopardy assessment, levy and distraint, and enforcement of liens).

Establishes within the Internal Revenue Service an office to be known as the Office of Taxpayer Services to be under the supervision and direction of an Assistant Commissioner of Internal Revenue who shall assist taxpayers in obtaining easily understandable tax information and answering questions on tax liability, among other functions.

States that, upon application filed by a taxpayer with

the Office of Taxpayer Services, in such form, manner, and at such time as the Secretary or his delegate shall by regulations prescribe, the Assistant Commissioner for Taxpayer Services may issue a Taxpayer Assistance Order if, in the determination of the Assistant Commissioner, the taxpayer is suffering from an unusual, unnecessary, or irreparable loss as a result of the manner in which the internal revenue laws are being administered by the Secretary or his delegate.

Authorizes the President of the Legal Services Corporation to establish Taxpayer Representation Offices in four cities selected by such President for purposes of providing legal assistance to individuals in connection with: (1) any audit by the Service of any return made by or on behalf of the individual with respect to any tax imposed by chapter 1 of the Internal Revenue Code of 1954, or (2) an assessment or collection from any such individual of any tax imposed by such chapter.

Provides for show cause hearings with respect to jeopardy assessments and termination of taxable years.

Increases the monetary value of specified items to be exempt from levy.

Provides criminal penalties (a fine of up to $10,000, or imprisonment for up to 2 years or both) for investigations into or surveillance over the beliefs, associations, or activities of any individual or organization which are not directly related to such revenue laws. Provides a civil cause of action for damages or an injunction, or both, for such violations.

Prohibits inspection of tax returns pursuant to a criminal investigation unless a search warrant has issued upon probable cause to believe that no alternative source of necessary information is available.

Provides rules for civil investigation related to: (1) payment of Social Security and Railroad Retirement taxes; (2) pension administration; (3) census information; (4) enforcement of taxpayers' rights under this Act; (5) inspection by States; (6) inspection by Committees of Congress; and (7) disclosure to persons having substantial interest (agents of partnerships and corporations, and shareholders of corporations).

Provides a civil action for damages for unauthorized disclosure of tax information.

S. 2380. Mr. Weicker; 9/19/75. Finance.

Taxpayer Privacy Act - Prohibits, generally, disclosure of tax returns or return information by officers or employees of the United States or any State.

Authorizes disclosure of income tax returns to specified persons and entities including: (1) the taxpayer for whom the return was made or his attorney in fact; (2) officers and employees of Federal and State agencies charged with the administration and enforcement of the tax laws; (3) the Joint Committee on Internal Revenue Taxation; (4) shareholders owning outstanding stock of any corporation, in

the case of a return of the corporation; and (5) the President.

Authorizes disclosure to the taxpayer's agent in the case of the taxpayer's death or bankruptcy.

Provides criminal penalties of up to $10,000, imprisonment of up to five years, or both, for unauthorized disclosures by public employees, or unauthorized receipt of tax information by any person from a public employee, under this Act.

Provides an additional criminal penalty of $1,000 for unauthorized disclosure or receipt of a tax return or tax return information by any person.

S. 2757. Mr. McClellan; 12/9/75. , Hruska, Taft.

Extends from January 31, 1976, to April 30, 1976, the authority under the Omnibus Crime Control and Safe Streets Act, of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. [Amends 18 U.S.C. 2510 note]

12-09-75 Measure called up by unanimous consent in Senate
12-09-75 Measure considered in Senate
12-09-75 Measure passed Senate
12-10-75 Referred to House Committee on the Judiciary
12-15-75 Measure called up by committee discharge in House
12-15-75 Measure considered in House
12-15-75 Measure passed House
12-16-75 Measure enrolled in House
12-16-75 Measure enrolled in Senate
12-16-75 Measure presented to President
12-23-75 Public law 94-176

S. 3057. Mr. Schweiker; 3/1/76.
Banking, Housing and Urban Affairs, Church, Haskell, Humphrey, Scott (Pa.).

Amends the Truth in Lending Act to prohibit a credit card issuer from providing any records or information relating to a cardholder's use of that issuer's credit card to a third party without the consent of the cardholder.

Requires that a credit card issuer notify the cardholder of the receipt of a subpena before it can provide any information pursuant to such subpena.

S. 3197. Mr. Kennedy; 3/23/76. Judiciary, Bayh, Byrd (W. Va.), Hruska, Mathias, McClellan, Nelson, Scott (Pa.).

Foreign Intelligence Surveillance Act - Requires the Chief Justice of the United States to designate seven district court judges, each of whom shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States. Requires the Chief Justice to designate three Federal judges to comprise a special court of appeals which shall have

jurisdiction to hear an appeal by the United States from the denial of any application. Grants the United States a further right to appeal an affirmance of denial to the Supreme Court

Requires each application for any order approving electronic surveillance for foreign intelligence purposes to be approved by the Attorney General and to include: (1) the identity of the officer making the application; (2) the authority conferred on the applicant by the President and the approval of the Attorney General to make the application; (3) the identity of the subject of the surveillance; (4) the fact and circumstances justifying belief that the target of surveillance is a foreign power or an agent of a foreign power; (5) a description of the type of information sought and a certification by one of specified Federal officers that such information is foreign intelligence information that cannot feasibly be obtained by normal investigative techniques; and (6) a statement of the period of time for which the surveillance is required.

Directs the judge to enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that the criteria specified have been met. Allows issuance of orders to approve surveillance for 90 days or the period necessary to achieve its purposes, whichever is less. Permits extensions of orders upon application for an extension made in the same manner as required for an original application.

Authorizes the Attorney General, upon a reasonable determination that an emergency situation exists, to authorize the emergency employment of electronic surveillance if the appropriate judge is informed by the Attorney General of such authorization at the time it is made and if an application is made as soon as practicable but not more than 24 hours after authorization. Requires, in the absence of a judicial order, that surveillance terminate when the information sought is obtained, when the application for an order is denied, or 24 hours after authorization, whichever is earliest.

Allows information acquired from electronic surveillance conducted pursuant to this Act to be used and disclosed only for designated purposes or for the enforcement of the criminal law.

Requires, when an order to approve the emergency employment of electronic surveillance is not obtained, that the judge serve notice on the individual subject to surveillance of the fact of the application, the period of surveillance, and the fact that information was or was not obtained. Permits the judge to delay or forego this action on a showing of good cause.

Requires the Attorney General to submit an annual report to the Administrative Office of the United States Courts and to Congress including: (1) the number of applications made for orders and extensions of orders approving electronic surveillance and the number of such orders and extensions granted, modified, and denied; (2) the periods of time for which orders authorized surveillances and their actual

duration; (3) the number of surveillances in place at any time during the preceding year; and (4) the number of surveillances terminated during the preceding year.

Declares that nothing contained in this Act shall limit the Constitutional power of the President to order electronic surveillances for specified national security reasons if the facts and circumstances giving rise to such order are beyond the scope of this Act. [Amends 18 U.S.C. 2521-2528]

S. 3349. Mr. Mathias; 4/29/76. Judiciary, Bayh, Leahy, Mathias, Nelson, Ribicoff, Tunney.

Bill of Rights Procedures Act - Title I: Confidentiality of Financial, Toll, and Credit Records - Prohibits any United States entity or representative from obtaining copies of, or access to, information contained in the financial records, toll records, or credit records of any customer of a financial institution, communication common carrier, credit card issuer, or consumer reporting agency. Removes such prohibition if the records are described with sufficient particularity, if the customer has authorized disclosure, and if disclosure is obtained in response to an administrative supoena, search warrant, or judicial subpoena.

Sets forth procedures for obtaining customer authorization, administrative subpoenas and summons, search warrants, and judicial subpoenas.

Requires financial institutions, communication common carriers, credit card issuers, and consumer reporting agencies to keep records of all examinations of customer records, including the identity of the person examining such records, the governmental agency or department such person represents, and a copy of the authorization.

Stipulates that any action under this title may be brought in any appropriate U.S. district court without regard to the amount in controversy, or in any other court of competent jurisdiction, within three years from the date on which the violation occurs or the date of discovery of such violation, whichever is later.

Imposes liability on any person or entity who knowingly obtains or discloses information in violation of this title, making such person or entity liable to the customer to whom the disclosed information relates for actual damages, such punitive damages as the court may allow if the violation was willful, and the costs of litigation. Makes injunctive relief available to any person aggrieved by a violation or threatened violation of this Act.

Title II: Mail Covers - Defines a "mail cover" as the procedures initiated at the request of a law enforcement authority by which a systematic inspection is made of any data appearing on the outside cover of any mail matter.

Prohibits the initiation of any mail cover without the written authorization of specified postal officials and good cause to believe, on the basis of an affidavit setting forth the specific reasons for the proposed mail cover, that such

procedure is necessary to the investigation of commission or attempted commission of a felony or is necessary to aid in locating a fugitive

Permits a mail cover to be conducted for 30 days with extensions to be granted as specified. Requires any mail cover conducted for more than one year to be judicially authorized. Allows the chief postal inspector or a regional chief postal inspector to issue an emergency authorization for a mail cover on the basis of an oral request from specified law enforcement officials, if such request is supported by an affidavit within 45 days and on condition that no data from such mail cover be made available to the requesting authority until authorization according to regular procedures has been granted.

Stipulates that the subjects of mail covers shall be given notice of such cover within 90 days of its termination, unless notice is judicially waived due to possible jeopardizing of continuing investigations.

Requires that the chief postal inspector submit to Congress an annual report including the number of requests for mail covers, the identity of the law enforcement agencies making such requests, and a list of the offenses for which mail cover requests were received.

Title III: Amendments to Chapter 119, Title 18, United States Code - Sets forth procedures and restrictions governing the interception of wire or oral communications for purposes of supervisory observing or service by communication common carriers and others. Requires each communication common carrier to submit an annual report to the Federal Communications Commission detailing the interceptions made by it for the protection of its service against theft of service, the nature and frequency of communications intercepted, the number of persons whose communications were intercepted, the length of such interceptions, and the number of hours of recording of intercepted communications.

Prohibits the manufacture, distribution, possession, and advertising of devices for theft of communication common carrier services. Stipulates that any such device may be seized and forfeited to the United States.

Title IV: Penalties - Subjects officers, agents, or employees of the United States who violate any provision of title I or title II of this Act to a fine of not more than $1,000, imprisonment for not more than one year, or both.

Title V: Congressional Subpoenas - Stipulates that nothing in this Act shall apply to Congressional subpoenas.

S. 3405. Mr. Curtis; 5/11/76. Finance.

Amends the Internal Revenue Code to provide that tax returns and tax reform information shall be confidential and shall not be disclosed under any circumstances except to such persons and for such purposes as are authorized by this Act.

Provides that returns and return information, except with regard to taxes imposed on wagering and machine guns,

shall be available to State tax agencies to the extent necessary for the administration of a specific tax law of a State and shall be used only for tax administration.

Provides for disclosure of returns and information to the House Ways and Means Committee, the Senate Committee on Finance, and the Joint Committee on Internal Revenue Taxation upon written request of the chairman of the Committee for use in closed executive session.

Authorizes disclosure to other Congressional committees upon written request of the chairman for use in closed executive session if the committee is authorized by a resolution of the House or Senate to inspect returns or return information.

Authorizes the disclosure of returns and return information to the President if he submits to the Secretary of the Treasury a written request containing specified information.

Provides for the disclosure of returns and return information to Federal officers and employees directly engaged in the preparation of any Federal administrative or judicial proceeding pertaining to the enforcement of a specific Federal statute not involving tax administration only if: (1) the taxpayer is or may be a party to such proceeding; (2) the taxpayer consents; or (3) the return or return information has a direct bearing on the outcome of such proceeding because of the existence of specified relationships between parties to the proceedings and the taxpayer.

Authorizes the disclosure of returns and return information in any Federal or State judicial or administrative proceeding pertaining to tax administration or any judicial or administrative proceeding pertaining to a specified Federal statute not involving tax administration if: (1) the taxpayer is a party to such proceeding; (2) the taxpayer consents; (3) the return or return information may have a direct bearing on the outcome of such proceeding; (4) it is necessary to impeach the testimony of the taxpayer as a witness; (5) it is required by the Federal Rules of Criminal Procedure; (6) it is required by the United States Constitution.

Provides for disclosure of specified return information to specified Federal agencies and officials if an individual is under consideration for appointment to a position in the executive or judicial branch of the Federal Government.

Authorizes disclosure of taxpayer identity information to any Federal agency and to State and local welfare agencies for purposes of locating an individual with respect to whom a return has been filed.

Provides that return information may be disclosed to the Justice Department to the extent necessary to answer an inquiry as to whether a juror in a Federal proceeding has, or has not, been investigated by the Treasury Department.

Authorizes the disclosure of return information pertaining to violations of criminal laws to the Attorney General and to States.

Directs the Secretary of the Treasury to maintain a

79-064 O - 76 - 49

record of all requests for inspection or disclosure of returns and return information, and of returns and return information inspected or disclosed under this Act.

Provides that disclosures of returns or return information in violation of this Act shall be punished by a fine of not more than $5,000, or imprisonment for not more than one year, or both. Requires dismissal of the offender if he is an officer or employee of the United States.

S. 3435. Mr. Ribicoff; 5/13/76.

Authorizes to be appropriated to carry out the provisions establishing the Privacy Protection Study Commission of the Privacy Act of 1974 $2,000,000 for fiscal years 1976 and 1977 without fiscal year limitation (previously $1,500,000 was authorized to be appropriated for fiscal years 1975, 1976 and 1977 with a $750,000 expenditure limit for any one fiscal year).

5-13-76	Reported to Senate from the Committee on Government Operations, S. Rept. 94-861
5-13-76	Placed on calendar in Senate
5-19-76	Call of calendar in Senate
5-19-76	Measure considered in Senate
5-19-76	Measure passed Senate
5-20-76	Referred to House Committee on Government Operations

S. 3559. Mr Brock; 6/14/76.
Banking, Housing and Urban Affairs.

Credit Information Protection Act - Amends the Consumer Credit Protection Act to prohibit any employee, officer, or agent of the United States from obtaining information contained in the credit records of any credit card issuer with respect to an identifiable credit and customer unless the procurement of such information is permitted by the informed written consent of such customer or is obtained by a search warrent or subpeona issued in accordance with the procedures required by this Act.

States that if a subpeona is used to obtain such information, the customer to whom such records relate must be sent a copy of such subpoena and must be given 18 days in which to respond to prevent such obtainment. Provides that notice to such customer of a judicial subpeona may be delayed if a United States court finds that such notification would seriously jeopardize a continuing investigation of specified criminal offenses including murder, kidnapping, robbery, or extortion.

Requires a judge granting such delay to report within 30 days after the expiration of such delay to the Administrative Office of the United States Courts with respect to the reasons for such delay.

Prohibits transfering from one Federal agency to any other information obtained pursuant to this Act in the absence of specific legislation authorizing such transfer.

Permits any person injured by anyone in violation of this Act to sue for actual damages, punitive damages if such violation was willful, and costs of bringing such suit including reasonable attorney's fees.

BILLS AND RESOLUTIONS - 94th CONGRESS

HOUSE BILLS

H. R. 61. Mr. Edwards (Calif.); 1/14/75. Judiciary.

Criminal Justice Information Control and Protection of Privacy Act - Title I: Purpose and Scope - Expresses the findings of Congress and the basis for this Act. Defines the terms used in this Act and the criminal justice agencies to which this Act applies, including agencies which exchange information interstate. Specifies the records and proceedings to which this Act does not apply, including court records of public criminal proceedings.

Title II: Collection, Dissemination, and Use of Criminal Justice Information - Requires criminal justice agencies to publish regulations specifying the type of information systems maintained, the limits on use of such information, and additional enumerated regulations. Requires the adoption of specified protective internal operating procedures by such agencies. Places the same limitations on data obtained from a foreign government.

States that identification information may be disseminated for official purposes but when such information includes arrest record or criminal record information, dissemination shall be only as permitted by this Act.

Prescribes procedures governing: (1) access to automated criminal justice information systems, which shall be by formal written agreements; (2) dissemination, access, and use by noncriminal justice agencies; (3) access for appointments and employment investigations; and (4) secondary use of criminal justice information.

Requires each agency to adopt procedures to insure physical security, continued accuracy, corrections and information, and periodic reviews.

Outlines the procedures for access by individuals for purpose of challenges

States that criminal justice intelligence and investigative information may be collected by a criminal justice agency only for offical purposes. Enumerates the internal operating procedures to be adopted by such agencies

Title III: Administration and Enforcement - Establishes in the executive branch the Commission on Criminal Justice Information, describing its powers and duties, including to appraise the laws, policies and practices of Federal, State and local governments with respect to criminal justice information systems.

Requires each agency to adopt procedures relating to administrative sanctions

Provides judicial remedies to individuals denied access to information concerning themselves in violation of this Act. Declares that any State or local agency participating in a criminal justice information system subject to this Act shall be deemed to have consented to the bringing of actions under this Act.

Authorizes to be appropriated funds necessary to carry

out the provisions of this Act.

H. R. 62. Mr. Edwards (Calif.); 1/14/75, Judiciary.

Criminal Justice Information Control and Protection of Privacy Act - Title I: Findings and Declaration of Policy; Definitions; Applicability - Declares that in order to insure the security of criminal justice information systems, and to protect the privacy of individuals named in such systems, it is necessary and proper for the Congress to regulate the exchange of such information. Sets forth the definitions of terms used in this Act. Describes the information systems to which this Act applies, including those operated by the Federal Government, and to which it does not apply, including original books of entry or police blotters.

Title II: Collection and Dissemination of Criminal Justice Information, Criminal Justice Investigations Information and Criminal Justice Intelligence Information - Prescribes the procedures for: (1) dissemination, access, and use of criminal justice information by criminal justice agencies; (2) dissemination of identification record and wanted persons record information; (3) dissemination, access, and use of criminal justice information by noncriminal justice agencies; and (4) dissemination, access, and use of criminal justice information with respect to appointments and employment investigations.

Prohibits agencies having access to criminal justice information from disseminating it to others not authorized to have it or from using it for a purpose not authorized by this Act, with limited exceptions with regard to rehabilitation officials.

Places limitations on access to criminal justice information via categories other than name.

Requires every agency information system covered by this Act to promulgate regulations on security, accuracy, updating and purging. Sets out what such regulations must provide. Requires every agency or information system to establish a process for access and challenge of incorrect or inaccurate information. Details what such regulations must provide.

Places limitations on the collection and dissemination of intelligence information. States that such information may not be maintained in automated systems and must be kept separate and apart from all other criminal justice files.

Enumerates the conditions under which criminal justice investigative information may be disclosed.

Title III: Administrative Provisions; Regulations; Civil Remedies; Criminal Penalties - Creates a Criminal Justice Information Systems Board to have responsibility for the administration and enforcement of this Act.

Requires each State to establish a central administrative agency, separate and apart from existing

criminal justice agencies, with authority to oversee operation of criminal justice information systems in that State.

Requires every information system or agency to give public notice, once annually, of the type of information it collects and disseminates, its sources, purpose, administrative director and other pertinent information.

Requires audits of systems and agencies which collect and disseminate information. States that such audits are to be conducted by the Board, by the State agency, and by each criminal justice system.

Permits the Federal Government to operate an interstate criminal justice information system under the policy control of the Board. Limits information contained in such system.

Lists administrative actions that may be taken by the Board in the event that a criminal justice information system is found to have violated any provision of this Act.

Provides the judicial machinery for the exercise of the right granted in this Act. Provides that aggrieved individuals may obtain both injunctive relief and damages, $100 recovery for each violation, actual and general damages, and attorney's fees.

Provides criminal penalties for violations of this Act.

Provides that any State regulation which imposes stricter privacy requirements on the operation of criminal justice information systems or upon the exchange of criminal justice information takes precedence over this Act or any regulations issued pursuant to this Act.

Authorizes the appropriation of such funds as the Congress deems necessary for the purposes of this Act.

H. R. 141. Mr Kastenmeier; 1/14/75. Judiciary.

Surveillance Practices and Procedures Act - Defines the term "foreign agent" for purposes of permissible wire interceptions and interceptions of communications as meaning a person who is engaged in activities which, in the opinion of the Attorney General, are intended to serve the interests of a foreign principal and undermine the security or national defense of the United States. Defines the term "foreign principal" for purposes of this Act.

Requires that in January, April, July, and October of each year, the Attorney General shall report to the Committees of the Judiciary and on Foreign Relations of the Senate and the Committees on the Judiciary and on Foreign Affairs of the House of Representatives specified information with respect to interceptions of wire or oral communications made during the preceding 3 months pursuant to applications made, and orders and extensions granted or denied, for legal wire interceptions.

Directs the President, the Attorney General, and all departments and agencies of the United States to supply to any committee named in this Act, upon request of such committee, any information regarding any interception of wire or oral communications covered by this Act, within 30 days after the receipt of such request.

H. R. 142. Mr. Kastenmeier; 1/14/75. Judiciary.

Freedom from Military Surveillance Act - Restricts the actions of any civil officer of the United States or any member of the Armed Forces of the United States in using the Armed Forces of the United States to exercise surveillance of civilians or to execute the civil laws.

Sets forth penalties for violations of the provisions of this Act.

H. R. 169. Ms. Abzug; 1/15/75. Government Operations.

Allows an individual, after a personal review of a record pertaining to him maintained by an agency of the Federal Government and permission to amend such record, the right to correct, expunge, update, or supplement any portion which the individual believes is not accurate, relevant, legally maintained, timely, or complete.

Provides that the records maintained by the Central Intelligence Agency or in connection with providing protective service to the President or Vice President shall not be exempted from the requirements of the Privacy Act of 1974.

H. R. 171. Ms. Abzug; 1/14/75. Judiciary.

Prohibits the interception of wire or oral communications unless all parties to the intercepted communication consent. [Amends 18 U.S.C. 2511]

H. R. 214. Mr. Mosher; 1/14/75. Judiciary.

Bill of Rights Procedures Act - States that it is the purpose of this Act to prohibit any interception of communication, other electronic surveillance, surreptitious entry, mail opening, or the inspection of and procuring of the records of telephone, bank, credit, medical, or other business or private transactions, of any individual without a court order issued upon probable cause that a crime has been or is about to be committed, supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.

Provides that whoever, being an officer, agent, or employee of the United States or any department or agency thereof willfully: (1) searches any private dwelling used and occupied as a dwelling without a warrant directing such search or maliciously and without reasonable cause searches any other building or property without a search warrant; (2) procures or inspects the records of telephone calls, bank, credit, medical, or other business or private transactions of any individual without a search warrant or the consent of the individual; (3) opens any foreign or domestic mail not directed to him without a search warrant directing such opening or without the consent of the sender or addressee of such mail; or (4) intercepts, endeavors to intercept, or procures any other person to intercept any wire or oral

communication except as authorized by law; shall be fined not more than $10,000 or imprisoned not more than one year, or both.

Requires that within 30 days after the date of an order authorizing or approving the interception of a wire or oral communication (or each extension thereof) entered under authority of law, or the denial of an order approving an interception, the person seeking such order shall report to the Administrative Office of the United States Courts and to the Committees on the Judiciary of the Senate and House of Representatives: (1) the fact that an order or extension was applied for; (2) the kind of order or extension applied for; (3) the fact that the order or extension was granted as applied for, was modified, or was denied; (4) the period of interceptions authorized by the order, and the number and duration of any extensions of the order; (5) the names of all parties to the intercepted communications; (6) the offense specified in the order or application; (7) the identity of the investigative or law enforcement officer and agency making the application and the person authorizing the application to be made; (8) a copy of the court order authorizing, approving, or denying such interception; and (9) the nature of the facilities from which or the place where communications were intercepted.

Specifies that reports be made within 90 days after the date of an order approving the interception of a wire or oral communication on the disposition of all records of any such interception and the identity of and action taken by all individuals who had access to any such interception.

Sets forth reporting requirements in the case of warrants issued authorizing the opening of mail.

H. R. 215. Mr. Kastenmeier; 1/14/75. Judiciary, Cohen, Railsback.

News Source and Information Protection Act - Provides that no newsman be required in any State or Federal proceeding to disclose information or the identity of a source of information received or obtained by him in his capacity as a newsman except as qualified by this Act.

Declares that any order of a State or United States court pertaining to a claim of privilege on the part of a newsman is subject to judicial review. Provides that appeals be heard at the earliest practicable date.

States that this Act should not be construed to impair any State law which secures the minimum privileges established by this Act.

Provides that the protection afforded by this Act not be available to a defendant in a defamation suit with respect to the source of any allegedly defamatory information which such defendant asserts a defense based on such source.

Declares that if any provision of this Act is declared invalid, the remainder shall not be affected thereby.

H. R. 266. Mr. Boland; 1/14/75. Judiciary.

Freedom from Military Surveillance Act - Restricts, the actions of any civil officer of the United States or any member of the Armed Forces of the United States in using the Armed Forces of the United States to exercise surveillance of civilians or to execute the civil laws.

Sets forth penalties for violations of the provisions of this Act.

H. R. 388. Mr. Chappell; 1/14/75. Judiciary.

Authorizes the Attorney General to exchange criminal record information with State and local agencies, where such State and local agencies are authorized by their laws and regulations to acquire such information in the performance of their official duties and functions.

H. R. 414. Mr. Fish; 1/14/75. Judiciary.

See Digest of H. R. 214.

H. R. 533. Mrs. Holt; 1/14/75. Ways and Means.

Restricts the authority for the inspection of income tax returns to specified persons and entities, including: (1) the taxpayer for whom the return was made or his attorney in fact; (2) officers and employees of Federal and State agencies charged with the administration and enforcement of the tax laws; (3) Committees of the Congress pursuant to a resolution of the House or Senate; and (4) shareholders of record owning one percent or more of the outstanding stock of any corporation.

H. R. 539. Ms. Holtzman; 1/14/75. Judiciary.

Freedom from Surveillance Act - Prohibits any civil or military officer of the United States or the militia of any State from exercising surveillance of civilians.

Provides a fine of not more than $10,000, imprisonment for not more than two years, or both, for civil or military officers convicted of violations of this Act.

Sets forth exceptions to the prohibitions of this Act and defines terms used in this Act.

Authorizes any person aggrieved as a result of conduct prohibited by this Act to bring a civil action for damages irrespective of the actuality or amount of pecuniary injury suffered. Allows a person to seek injunctions to prevent violations of this Act.

H. R. 550. Mr. Koch; 1/14/75.
Banking, Currency and Housing.

States the finding of the Congress that: (1) procedures and policies governing the relationship between fiduciary institutions and government agencies have in some cases developed without due regard to the constitutional rights of customers of those institutions; (2) the confidential

relationships between fiduciary institutions and their customers must be preserved and protected; and (3) certain reporting and recordkeeping requirements imposed on fiduciary institutions by government agencies constitute a burden on interstate and foreign commerce.

Provides that a fiduciary institution may not disclose to any person except to the customer or his duly authorized agent any financial records relating to that customer of that fiduciary institution unless: (1) such customer has authorized, in accordance with this Act, disclosure to such person; or (2) such financial records are disclosed in response to a court order which meets the requirements of this Act.

Sets forth the conditions for authorization of disclosure of records as required for this Act. Provides for recordkeeping requirements under this Act.

Sets forth civil penalties for violations of this Act. Provides that any fiduciary institution which knowingly and willfully discloses financial records in violation of this Act shall be liable to the customer to whom such records relate in an amount equal to the sum of: (1) any actual damages sustained by the person as a result of the failure; (2) such punitive damages as the court may allow, except that such punitive damages shall be not less than $100; and (3) in the case of any successful action to enforce liability under this section, the cost of the action together with reasonable attorneys fees as determined by the court.

Sets forth criminal penalties for violations of this Act. Provides that whoever, being an officer or employee of a fiduciary institution, knowingly and willfully furnishes financial records in violation of this Act shall be guilty of a misdemeanor, and upon conviction shall be imprisoned for not more than one year or fined not more than $5,000 or both.

Provides that whoever knowingly and willfully induces or attempts to induce any officer or employee of a fiduciary institution to disclose financial records in violation of this Act, is guilty of a misdemeanor and upon conviction shall be imprisoned for not more than one year or fined not more than $5,000, or both.

H. R. 562. Mr Koch; 1/14/75. Judiciary.

Provides that a person connected with or employed by the news media cannot be required by a court, legislature or administrative body to disclose before the Congress or any Federal court or agency, information or the source of any information procured for publication or broadcast.

H. R. 564. Mr. Koch; 1/14/75. Judiciary.

States that it shall be unlawful for any officer or employee of any executive department or agency to do the following: (1) to require or request any officer or employee of the United States, or any individual applying for

employment as an officer or employee of the United States, to take any polygraph test in connection with his services or duties or in connection with his application for employment; or (2) to discharge, discipline, or deny promotion to any officer or employee of the United States, or to threaten to commit any such act by reason of his refusal or failure to submit to such requirement or request.

Provides that it shall be unlawful for any person engaged in any business or other activity in or affecting interstate commerce to do the following: (1) to require or request any officer or employee or any individual applying for employment to take any polygraph test; or (2) to deny employment to any individual, or to discharge, discipline, or deny promotion to any officer or employee, or to threaten to commit such act, by reason of his refusal or failure to submit to such requirement or request.

Sets forth criminal penalties for violations of the provisions of this Act.

H. R. 616. Mr. Litton; 1/14/75. Ways and Means.

Prohibits, except as provided in this Act, the inspection of tax returns and the disclosure of information contained in such returns. Authorizes the inspection of returns by or disclosure to (1) the taxpayer or his representative; (2) employees of the Internal Revenue Service and Department of Justice solely for purposes of enforcement of the tax laws; (3) State agencies charged with administration of the tax laws only for that purpose; (4) the President of the United States in the performance of his official duties; and (5) the Joint Committee on Internal Revenue Taxation for statistical purposes only.

Increases the criminal penalties for unauthorized disclosure or receipt of information under this Act.

H. R. 620. Mr. Long (Md.); 1/14/75. Judiciary, Brown (Calif.), Chisholm, Collins (Ill.), Diggs, Harrington, Hechler, Helstoski, Mink, Mitchell (Md.), Moss, Rangel, Riegle, Wilson (Tex.).

Provides that it shall not be unlawful for a person to electronically record or otherwise intercept a wire or oral communication where all parties to such communication have given prior consent unless the interception is for the purpose of criminal or tortious act.

H. R. 623. Mr. Lujan; 1/14/75. Education and Labor.

Prohibits under the provisions of the General Education Provisions Act, the funding of grants to States, local educational agencies, and educational institutions which have a policy of denying, or which effectively prevent, teachers and other specified school employees the right to inspect and review any official records, files and data directly related to such teachers and employees.

Prohibits such funding where the States, agencies, or

institutions have a policy of permitting the release of personally identifiable records and files of teachers and specified employees without their written consent or without complying with the excpetions enumerated in this Act.

Requires the Secretary of Health, Education, and Welfare to establish or designate an office and review board to investigate and adjudicate violations under this Act.

H. R. 720. Mr. Murphy (N. Y.); 1/14/75.
Post Office and Civil Service.

Makes it unlawful for any executive branch officer or any person acting under such officer's authority to require employees or applicants for Government employment to: (1) disclose their race, religion, or national origin; (2) attend Government-sponsored meetings and lectures or participate in outside activities unrelated to their employment; (3) report on their outside activities or undertakings unrelated to their work; (4) submit to questioning about their religion, personal relationships or sexual attitudes through interviews, psychological tests, or polygraphs; and (5) support political candidates or attend political meetings. Permits inquiries into national origin when necessary for the national interest or overseas work. Allows agency officers to advise employees of charges of sexual misconduct as long as the employee has an opportunity to refute the charge.

Makes it illegal to coerce an employee to buy bonds or make charitable contributions; or to require him to disclose his own personal assets, liabilities, or expenditures, or those of any member of his family unless they would show a conflict of interest.

Provides a right to have counsel or other person present, if the employee wishes, at an interview which may lead to disciplinary proceedings.

Accords the right to a civil action in a Federal court for violation or threatened violation of this Act.

Directs the Attorney General to defend all persons sued who acted pursuant to an order or who, in his opinion, did not willfully violate this Act.

Establishes a three-member Board on Employees' Rights with members appointed by the President by and with the advice and consent of the Senate. Grants the Board the authority and duty to receive and investigate written complaints from any person claiming to be aggrieved by any violation or threatened violation of this Act and to conduct a hearing on each such complaint. Directs the Board to make an annual report of its activities to Congress.

Excludes the Federal Bureau of Investigation, the Central Intelligence Agency, and the National Security Agency from the provisions of this Act.

Permits the establishment of agency grievance procedures to enforce this Act, but provides that the existence of such procedures shall not preclude the use of other remedies.

H. R. 955. Mr. Roe; 1/14/75. Ways and Means.

States that all returns made with respect to the taxes imposed by the Internal Revenue Code are confidential records. Provides that: (1) no such return shall be open to inspection; and (2) no information contained in any such return shall be disclosed.

Authorizes inspections by the following persons: (1) the taxpayer or his authorized representative; (2) officers and employees of the Internal Revenue Service, Department of the Treasury, Department of Justice, and State and local government employees solely for purposes of enforcement and administration of the tax laws; and (3) the President of the United States in the necessary performance of his official duties.

Increases the criminal penalties for unauthorized disclosure of information under the provisions of the Internal Revenue Code.

States that any person who knowingly receives any information or material which is disclosed or furnished in violation of the provisions of this Act shall be guilty of a felony and subject to a fine of up to $10,000, imprisoned for up to five years, or both.

H. R. 1005. Mr. Rousselot; 1/14/75.
Banking, Currency and Housing.

Right to Financial Privacy Act - States that the purposes of this Act are to protect and preserve the confidential relationship between financial institutions and their customers and the constitutional rights of those customers, and to promote commerce by prescribing policies and procedures to insure that customers have the same right to protect against unwarranted disclosure of customer records as if the records were in their possession.

Prohibits any Federal agency or employee, or any State or local government, from obtaining copies of, access to, or the information contained in, the financial records of any customer from a financial institution unless the financial records are described with particularities and: (1) such customer has authorized such disclosure in accordance with this Act; (2) such financial records are disclosed in response to an administrative subpena or summons; (3) such financial records are disclosed in response to a court order; or (4) such financial records are disclosed in response to a judicial subpena.

States that no financial institution may provide to a Federal agency or employee, or to any State or local government, copies of or the information contained in the financial records of any customer except in accordance with the requirements of this Act.

Sets forth provisions governing customer authorization, administrative subpenas and summons, and judicial subpenas.

Provides that the Secretary of the Treasury may not require an institution to maintain any financial records or to transmit any reports relating to customers unless: (1)

such records are required for use by a supervisory agency in the supervision of that institution; or (2) such records are required to be maintained by the Internal Revenue Code.

Prescribes civil and criminal penalties for violation of the provisions of this Act.

H. R. 1098. Mr. Teague; 1/14/75. Government Operations.

Provides that individuals be apprised of records concerning them which are maintained by Government agencies. Requires each agency to notify such individuals by mail of such records, maintain an accurate record of the names of all persons inspecting such records, refrain from disclosing the record without permission, permit any individual to inspect his record and permit the individual to supplement the information which he deems pertinent to his record. [Adds 5 U.S.C. 552a]

Excludes from the provisions of this Act those records required by executive order to be kept secret, investigatory files compiled for law enforcement purposes, and agency memorandums not available to a party in litigation with an agency.

H. R. 1173. Mr Wilson, Charles H.; 1/14/75.
Post Office and Civil Service.

Declares that it is the policy of the United States, as an employer, to assure that those officials of Executive agencies charged with administrative or supervisory responsibility recognize and protect the personal and individual rights, entitlements, and benefits of employees of, and applicants for employment in, Executive agencies.

Provides that an official of an Executive agency may not: (1) require or request an employee or an applicant for employment in an Executive agency to disclose his race, religion, or national origin, or the race, religion, or national origin of any of his forebears; (2) coerce, require, or request an employee to attend or participate in a formal or informal meeting, assemblage, or other group activity held to present, advocate, develop, explain, or otherwise cover in any way, any matter or subject other than the performance of the employee's official duties, or the development of skills, knowledge, or abilities that qualify him for the performance of those official duties; (3) coerce, require, or request any employee to participate in any way in an activity or undertaking unless it is related to the performance of the employees official duties, or to make any report concerning any activity or undertaking of the employee not involving his official duties; (4) require or request an employee, or any applicant for employment, to submit to an interrogation or examination or to take a polygraph or psychological test designed to elicit from the employee or applicant information concerning his personal relationship with any individual related to him by blood or marriage, his religious beliefs or practices, or his attitude or conduct with respect to sexual matters; (5)

coerce or require an employee to invest his earnings in bonds or other obligations or securities issued by the United States or by an Executive agency, or to make donations to any institution or cause of any kind, (6) require or request an employee to disclose his property or the property of any member of his family or household; (7) prohibit or restrict the exercise by an employee of the right of reasonable communication with an official of his agency; or (8) in any way remove or suspend an employee for refusal or failure of the employee to submit to or comply with any requirement, request, or action prohibited by the Act, or the exercise by the employee of any right, entitlement, benefit, or other protection granted or secured by the foregoing and the right to request judicial review in a Federal Court of actions against him provided by this Act.

Provides that the above shall not apply to: (1) the Central Intelligence Agency; (2) the National Security Agency; (3) the Federal Bureau of Investigation; or (4) any other Executive agency as the President in the interest of national security may recommend to the Congress.

Provides for a grievance procedure for an employee who claims to be aggrieved by a violation of this Act.

Establishes a Board on Employee Rights. Provides that the Board shall hear complaints from employees, or applicants for employment, on alleged violations of the provisions of this Act. Specifies the procedure under which the Board shall operate, including notice to all parties and a prompt hearing.

Empowers the Board to make final decisions on all such complaints for purposes of judicial review. Provides that, when an Executive agency is determined to be in violation of the Act, the Board shall have the power: (1) to issue cease and desist orders; (2) to use informal powers of conference, conciliation, and pursuasion; and (3) to issue an official reprimand to or suspend the pay for a maximum of 15 days of the official for his first offense, or suspend his pay for 15 to 60 days or order removal from office of the official for his second offense.

Provides that if the Board determines that a violation of this Act has been committed or threatened by an official of an Executive agency subject to the Uniform Code of Military Justice, the Board shall: (1) report such finding to the Secretary of the department involved; and (2) endeavor to eliminate any unlawful act or practice which constitutes such a violation by informal methods of conference, conciliation, and persuasion.

Provides that the Secretary of the department involved shall take immediate steps to dispose of the matter under the Uniform Code of Military Justice.

Provides that the Board shall make an annual report on its activities to the President for transmittal to Congress.

Provides that the Secretary of each military department shall submit an annual report to the President for transmittal to Congress on his activities under this Act. Provides that the Federal district court shall have the power to hear a petition for a review of a dtermination or

order of the Board, or a complaint for a trial de novo on the violation or threatened violation of this Act, which was the subject of the determination or order of the Board.

Provides that an individual called on to participate in any phase of an administrative or judicial proceeding under this Act shall be free from restraint, coercion, interference, intimidation, or reprisal in the course of, or because of, his participation.

H. R. 1185. Mr. Yates; 1/14/75. Armed Services.

Freedom from Surveillance Act - Restricts the authority of the Armed Forces to collect, distribute, and store information about civilian political activity and the activity of social or religious groups. Provides for criminal and civil actions for any violations of this Act.

H. R. 1324. Mr. Koch; 1/14/75.
Banking, Currency and Housing.

Provides that a person may not procure or cause to be prepared an investigative consumer report on any consumer unless it is clearly and accurately disclosed to the consumer that a report including information as to his character, general reputation, personal characteristics, and mode of living, whichever are applicable, may be made.

Requires that the disclosure: (1) be made in eight-point, boldface type in the application form for credit, employment, or insurance; and (2) include a statement informing the consumer of his right to request the additional disclosures.

Requires that the disclosure contain the name and address of the consumer reporting agency making the report. Provides that whenever a consumer reporting agency prepares a consumer report, it shall follow reasonable procedures to assure that only information relevant to the permissible purposes of the report is gathered and that such information is as accurate as possible.

Provides that a consumer reporting agency which compiles and reports items of information on consumers which are matters of public record shall: (1) at the time such public record information is reported to the user of the consumer report, notify the consumer of the fact that public record information is being reported by the consumer reporting agency, together with the name and address of the person to whom such information is being reported; and (2) maintain strict procedures designed to insure that whenever public record information is reported it is complete and up to date.

H. R. 1464. Mr. Pettis; 1/15/75. Government Operations.

Provides that no Federal agency may distribute, sell, or otherwise make available to any person any list of names and addresses of: (1) employees, or former employees, of any agency; (2) persons licensed by any agency; (3) persons

registered or required to file information with any agency; or (4) members, or former members, of the Armed Forces, except in accordance with the provisions of this Act.

Stipulates that an agency may make available a list of names and addresses of the persons referred to if the person to whom such list is made available certifies that: (1) such list will not be used for purposes of commercial or other solicitation; and (2) such list will not be used for any purpose which is unlawful under any State or Federal law.

States that any agency may make available a list of names and addresses if specifically authorized to do so by statute.

Provides that any person whose name and address is on any list made available by this Act and who is solicited in a communication mailed to him the address of which is obtained from such list may request the person who addressed such communication to remove his name from such list.

Sets forth penalties for violations of the provisions of this Act.

H. R. 1603. Mr. Drinan; 1/17/75. Judiciary.

Declares the finding of Congress that widespread wiretapping and electronic surveillance, both by private persons and Government agents under color of law and without pretense of legal excuse or justification, has seriously undermined personal security and often violated fundamental constitutional rights. Declares that no person in any branch of the Federal Government or in any other governmental or private position should be authorized either explicitly or implicitly to violate the constitutional rights of persons by eavesdropping on private conversations through wiretapping and electronic surveillance.

Removes the authority granted by Federal law to specified persons to legally intercept wire or oral communications and provides that no willful interception may be made without the consent of all the parties to such communications.

Prohibits specified persons, including the U. S. Attorney General, to seek court authorizations for interception of specified communications.

H. R. 1674. Mr. Daniels, Dominick V.; 1/20/75.
Post Office and Civil Service.

Entitles civilian employees of any executive department or any executive agency of the United States Government to the right to have a counsel or representative of his choice present during interrogations which may lead to disciplinary actions and to prevent unwarranted reports from employees concerning their private lives.

Provides for the filing of complaints of violations of this Act with the United States Civil Service Commission which shall have the power to enforce the provisions of this Act.

States that nothing contained in this Act shall be

construed to prevent the establishment of grievance procedures negotiated by labor organizations and agency managers which may be a substitute to the procedure provided by this Act.

Provides judicial review in a United States District Court for any party aggrieved by any final determination or order issued pursuant to this Act.

H. R. 1779. Mr. Bevill; 1/20/75. Ways and Means.

Prohibits, except as provided in this Act, inspection of tax returns and the disclosure of information contained in such returns

Authorizes the inspection returns by disclosure to: (1) the taxpayer or his representative; (2) employees of the Internal Revenue Service and Department of Justice solely for purposes of enforcement of the tax laws; (3) State agencies charged with administration of the tax laws only for that purpose; (4) the President of the United States in the performance of his official duties; and (5) the Joint Committee on Internal Revenue Taxation for statistical purposes only.

Increases the criminal penalties for unauthorized disclosure or receipt of information under this Act.

H. R. 1864. Mr. Kastenmeier; 1/23/75. Judiciary.

Freedom from Surveillance Act - Provides a penalty of a fine of not more than $10,000 or imprisonment for not more than one year, or both, for any U.S. civil officer who maintains surveillance over, or maintains records regarding the beliefs, associations, political activities, or private affairs any U.S. citizen, or regarding the beliefs, membership, or political activities of any group or organization of citizens

Provides that nothing in this Act shall be deemed either to limit or enlarge such legal authority of the United States as may exist to: (1) collect or maintain information relevant to an investigation of a person who has committed or is suspected on reasonable grounds to have committed a felony; and (2) collect and maintain information relevant to lawful investigations of persons who have applied for employment with the United States, who are employees, or who are contractors of prospective contractors of the United States.

Makes a civil officer who violates this Act liable for damages to any person, group, or organization that has been the object of conduct prohibited by this Act. Allows actual damages, punitive damages (not to exceed $1,000), and the costs of any successful action. Permits a class action in specified circumstances.

Allows a civil action to be brought in U.S. district courts, which shall have jurisdiction over such action without regard to the pecuniary amount in controversy.

Defines the terms used in this Act.

H. R. 1910. Mr. Matsunaga; 1/23/75.
Post Office and Civil Service.

See Digest of H. R. 1173.

H. R. 1984. Mr. Goldwater; 1/23/75. Judiciary, Koch.

Comprehensive Right to Privacy Act - Requires that any organization of State or local government maintaining an information system that includes personal information shall: (1) collect, maintain, use, and disseminate only personal information necessary to accomplish a proper purpose of the organization; (2) collect information to the greatest extent possible from the data subject directly; (3) maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject; (4) make no dissemination to another system or any individual other than the data subject without specifying requirements for security and the use of information exclusively for the purpose set forth in the notice required under this Act; (5) maintain a complete and accurate record, including identity purpose, and date, of every access to any personal information in a system by persons or organizations not having regular access authority; and (6) collect no personal information concerning the political or religious beliefs, affiliations, and activities of data subjects maintained by any government agency unless expressly authorized by statute.

Prohibits any State or local government from requiring individuals to disclose for statistical purposes any personal information unless such disclosure is required by a constitutional provision or Act of Congress, and the individual is so informed.

Requires any organization maintaining or proposing to establish an information system for personal information to: (1) give notice of the existence and character of each existing system once a year to the Federal Privacy Board; (2) give public notice of the existence and character of each existing system each year; and (3) assure that such public notice specifies the categories of data maintained, and the categories of all information sources, a description of types of use made of information, and the procedures whereby an individual can gain access to such information and contest its accuracy and the necessity for its retention.

Requires any organization maintaining personal information to inform an individual asked to supply personal information whether he is legally required, or may refuse, to supply the information requested, and also of any specific consequences, which are known to the organization, of providing or not providing such information.

Permits data subjects who dispute information about themselves to have such disputed information noted as being disputed when such information about him is disseminated. Requires, upon request, corrections in information to be

sent to past recipients of information.

Directs organizations maintaining information to inform, within two years and each year thereafter, individuals on whom data is stored of its content and where a copy of such data may be obtained.

Sets forth exemptions to the provisions of this Act.

Makes it unlawful for any organization to require an individual to disclose or furnish his social security account number, for any purpose in connection with any business transaction unless the disclosure or furnishing of such number is specifically required by Federal law.

Establishes the Federal Privacy Board whose five members shall be appointed by the President.

Directs the Board to: (1) publish an annual Data Base Directory of the United States containing the name and characteristics of each personal information system covered by this Act; (2) make rules to assure compliance with this Act; (3) upon the determination of a violation of a provision of this Act or regulation promulgated under the Act, and after opportunity for a hearing, order the organization violating such provision to cease and desist such violation; and (4) conduct open, public hearings on all petitions for exceptions or exemptions from provisions, application, or jurisdiction of this Act.

States that any individual or organization or responsible officer of an organization who willfully: (1) keeps an information system without having notified the Federal Privacy Board; or (2) issues personal information in violation of this Act; or (3) solicits, uses, or otherwise acquires information in violation of this Act shall be fined not more than $10,000 in each instance or imprisoned not more than five years, or both.

Provides that any person, system, or agency which violates the provisions of the Act, or any rule, regulation, or order issued thereunder, shall be liable to any person aggrieved thereby.

H. R. 2213. Mrs. Holt; 1/28/75. Education and Labor.

Provides, under the Equal Educational Opportunities Act, that no U.S. department, agency, officer, employee, or agent shall, as a prerequisite or condition to the receipt of Federal funds, require any school to provide access to any information or records which concern race, religion, sex, or national origin and which relate to: (1) public enrollments; (2) the employment or assignment of professional and other personnel; and (3) disciplinary actions or procedures.

Allows the Federal Government to seek access to such information by obtaining prior, voluntary, written consent of the school, or by submitting to an appropriate U.S. court a petition accompanied by affidavits by or on behalf of students or parents of students alleging unlawful discrimination by the school. Requires that the school be given reasonable notice and an opportunity for a hearing.

H. R. 2330. Mr. Mosher; 1/29/75. Judiciary, Abzug, Anderson (Calif.), Badillo, Conte, Conyers, Coughlin, Duncan (Tenn.), Forsythe, Harrington, Helstoski Holtzman, McCormack, McKinney, Moorhead (Calif.), Pettis, Quie, Regula, Roe, Ruppe, Sarasin, Seiberling, Stark, Talcott, Wilson, Charles H., Won Pat.

See Digest of H. R. 214.

H. R. 2453. Mr. Long (Md.); 1/30/75. Judiciary, Leggett.

See Digest of H. R. 620.

H. R. 2556. Mr. Wilson, Charles H.; 1/31/75. Post Office and Civil Service.

Authorizes the Secretary of Commerce to furnish, upon written request, authenticated copies of reports filed by, or on behalf of, an individual or organization to such individual or organization or to the heir or agent of such individual or organization.

Allows the Secretary to furnish copies of tabulations and other statistical materials which do not disclose the information reported by any individual or organization to any private person or agency requesting such information upon payment of the cost of such work.

Prohibits any officer or employee of the Federal Government from disclosing the names of individuals or the addresses of their residences as collected in the censuses without the written permission of such individuals or their heirs or authorized agents.

Directs the Secretary, in the year 1975 and every ten years thereafter, to conduct a mid-decade sample survey of population. Stipulates that information obtained in such mid-decade sample survey shall not be used for apportionment of Representatives in Congress among the several States.

Requires the Secretary to submit to the Congress for its recommendations for acceptance or rejection the questions proposed to be included in the decennial census and the mid-decade sample survey of population.

Authorizes the Secretary to conduct special censuses for the government of any State or any political subdivision within a State upon payment to the Secretary of the cost of such special census.

Increases the penalty for wrongful disclosure of census information by census employees from a fine of $1,000 and two years imprisonment to a fine of $5,000 and five years imprisonment. Extends such penalties to any officer or employee of the Federal Government who wrongfully discloses census information.

Repeals the provisions for imprisonment for refusal to answer questions and for making false answers to a census questionnaire.

Provides that if a provision enacted by this Act is held invalid, all valid provisions that are severable from the

invalid provision remain in effect.

H. R. 2566. Ms. Abzug; 2/3/75. Judiciary.

Freedom from Surveillance Act - Provides that whoever being a civil officer of the United States or an officer of the Armed Forces of the United States employs any part of the Armed Forces of the United States or the militia of any State to conduct investigations into, maintain surveillance over, or record or maintain information regarding, the beliefs, associations, or political activities of any person not a member of the Armed Forces of the United States, or of any civilian organization, shall be fined not more than $10,000, or imprisoned not more than two years, or both.

Excludes the provisions of this Act from the use of the Armed Forces of the United States or the militia of any State: (1) doing anything necessary or appropriate to enable such forces or militia to accomplish their mission after they have been actually and publicly assigned by the President to the task of repelling invasion or suppressing rebellion, insurrection, or domestic violence; or (2) investigating criminal conduct committed on a military installation or involving the destruction, damage, theft, unlawful seizure, or trespass of the property of the United States; or (3) determining the suitability for employment or for retention in employment of any individual actually seeking employment or employed by the Armed Forces of the United States or by the militia of any State, or by a defense facility; or (4) whenever the militia of any State is under the command or control of the chief executive of that State or any other appropriate authorities of that State.

Allows any person aggrieved as a result of any act which is prohibited by this Act to bring a civil action for damages irrespective of the actuality or amount of pecuniary injury suffered.

Allows any person who has reason to believe that a violation of this Act has occurred or is about to occur to bring a civil action on behalf of himself and others similarly situated against any civil officer of the United States or any military officer of the Armed Forces of the United States to enjoin the planning or implementation of any activity in violation of that section.

H. R. 2572. Mr. Aspin; 2/3/75.
Interstate and Foreign Commerce.

Telephone Privacy Act - Prohibits the making of unsolicited commercial telephone calls to persons who have notified their telephone company that they do not wish to receive such calls. Prescribes a $1,000 fine and/or thirty days imprisonment where at least ten written complaints of violations by any person have been received by the United States attorney in the judicial district.

H. R. 2596. Mr. Koch; 2/3/75. Judiciary.

States that it shall be unlawful for any officer or employee of any executive department or agency to do the following: (1) to permit, require, or request any officer or employee of the United States, or any individual applying for employment as an officer or employee of the United States, to take any polygraph test in connection with his services or duties or in connection with his application for employment; (2) to discharge, discipline, or deny promotion to any officer or employee of the United States, or to threaten to commit any such act by reason of his refusal or failure to submit to such requirement or request.

Provides that it shall be unlawful for any person engaged in any business or other activity in or affecting interstate commerce to do the following: (1) to permit, require, or request any officer or employee or any individual applying for employment to take any polygraph test; or (2) to deny employment to any individual, or to discharge, discipline, or deny promotion to any officer or employee, or to threaten to commit such act, by reason of his refusal or failure to submit to such requirement or request.

Sets forth criminal penalties for violations of the provisions of this Act.

H. R. 2603. Mr. Mosher; 2/3/75. Judiciary, Anderson (Ill.), Andrews (N. D.), Ashley, Bell, Brown (Calif.), Esch, Frenzel, Heinz, O'Brien, Pritchard, Richmond, Solarz, Symington, Whalen.

See Digest of H. R. 214.

H. R. 2604. Mr. Mosher; 2/3/75. Judiciary, Conlan, Goldwater, Heckler, Hinshaw, Horton, Lagomarsino, Thone.

See Digest of H. R. 214.

H. R. 2635. Ms. Abzug; 2/4/75. Government Operations, Conyers, Fascell, Gude, Rosenthal, Stanton, James V..

Allows an individual under the Privacy Act of 1974 to correct, expunge, update, or supplement such portion of a Federal records system as the individual believes is not legally maintained.

Repeals the exemption of the Central Intelligence Agency from specified requirements of the Privacy Act of 1974.

H. R. 2713. Mr. Pike; 2/4/75. Ways and Means.

States that the annual report of a private foundation required under the Internal Revenue Code need not include the names or addresses of needy or indigent recipients of charitable gifts or grants amounting to less than $1,000.

H. R. 2752. Mr. Stark; 2/4/75.
Banking, Currency and Housing.

Right to Financial Privacy Act - States that the purposes of this Act are to protect and preserve the confidential relationship between financial institutions and their customers and the constitutional rights of those customers, and promote commerce by prescribing policies and procedures to insure that customers have the same right to protection against unwarranted disclosure of customer records as if the records were in their possession.

Prohibits any Federal agency or employee, or any State or local government from obtaining copies of, access to, or the information contained in, the financial records of any customer from a financial institution unless the financial records are described with particularity and: (1) such customer has authorized such disclosure in accordance with this Act; (2) such financial records are disclosed in response to an administrative subpena or summons; (3) such financial records are disclosed in response to a court order; or (4) such financial records are disclosed in response to a judicial subpena.

States that no financial institution may provide a Federal agency or employee, or any State or local government, copies of or the information contained in the financial records of any customer except in accordance with the requirements of this Act.

Sets forth provisions governing customer authorization, administrative subpenas and summons and judicial subpenas.

Provides that the Secretary of the Treasury may not require an institution to maintain any financial records or to transmit any reports relating to customers unless: (1) such records are required for use by a supervisory agency in the supervision of that institution; or (2) such records are required to be maintained by the Internal Revenue Code.

Prescribes civil and criminal penalties for violation of the provisions of this Act.

H. R. 2753 Mr. Steelman; 2/4/75. Judiciary, Anderson (Ill.), Brown (Calif.), Edgar, Forsythe, Goldwater, Hefner, Horton, Keys, Koch, Martin, Mathis, Melcher, Mosher, Pritchard, Regula, Ryan, Solarz, Spence, Symington, Talcott, Thone Vigorito, Wilson (Tex.), Wilson, Charles H..

See Digest of H. R. 266.

H. R. 2754 Mr. Steelman; 2/4/75. Judiciary, Anderson (Calif.), Edwards (Calif.), Goldwater, Heckler, Horton, McKinney, Mitchell (Md.), Studds.

See Digest of H. R. 266.

H. R. 2819 Mrs. Holt; 2/5/75. Education and Labor, Eshleman, Gaydos, Jones (N. C.), Lott, McCollister, McDonald, Milford, Nichols, Symms,

Waggonner.

Prohibits any agency of the Federal Government, under the Equal Educational Opportunities Act, from requiring schools or other educational institutions, as a prerequisite to the receipt of Federal funds, to provide such agency with access to records concerning race, religion, sex, or national origin maintained by such schools, or other institutions, exept as provided in this Act.

H. R. 2862. Mr. Wilson, Charles H.; 2/5/75. Judiciary.

See Digest of H. R. 142.

H. R. 2885. Mr. Hamilton; 2/5/75. Ways and Means; Interstate and Foreign Commerce.

Requires the Secretary of Health, Education, and Welfare to assist the National Standards Review Council in proposing guidelines for selection of professional standards review areas, under the Medicare and Medicaid provisions of the Social Security Act.

Directs, after selection of such areas, that an agreement be entered into between the Secretary and a qualified organization which shall be the Professional Standards Review Organization (PSRO) for such area for five years.

Defines "qualified organizations" to include specified private nonprofit organizations and associations and public agencies.

Allows the Secretary to waive review and control activities under this Act where he finds effective review and control by PSROs.

Allows a majority of the doctors in an area to negate selection of a PSRO.

Establishes a trial period for a PSRO before it becomes fully responsible for review and control of medical services within its area.

Sets forth duties of PSROs, including review of medical services to determine: (1) if they were necessary; (2) if they meet professional standards; and (3) what inpatient services could be changed to outpatient services.

Limits physicians' reviews of patient services to those patients other than his own.

Allows PSROs to inspect physicians' records and facilities, where physicians and facilities provide services under this Act.

Requires a PSRO to rotate and provide the broadest possible inclusion of physicians doing reviewing for its area. Requires reviewing committees to demonstrate their capability before a PSRO must accept their findings.

Directs PSROs to identify or develop criteria of health care to be used for review and control in their areas.

Requires PSROs to report substantial violations of health care providers to the State-wide Professional Standards Review Council, but only after a chance for

voluntary compliance has been provided.

Prohibits the payment to providers of medical services who are with fault, as determined by the PSRO.

Sets forth an appeal procedure, through the National Standards Review Council, for such providers, where payment is refused them.

Obliges such providers to give necessary care, professional quality care, and inpatient care only where outpatient care will not suffice.

Provides for a suspension and thereafter an exclusion from services under this Act for providers not fulfilling such obligations Requires notice and opportunity of review for such providers of a decision to suspend or exclude.

Requires the establishment of State Councils where more than one PSRO exists in a State, in order to coordinate such PSROs. Requires that the membership of the State Councils include four public representatives.

Establishes the National Council, consisting of 15 physicians serving three-year terms, who will advise the Secretary, perform the duties specified under this Act, and review and seek to improve the operations of the PSROs.

Requires that State plans for provision of medical care under the Social Security Act meet the requirements of this Act.

Provides for the confidentiality of the records of PSROs and the State and National Councils, including patient records. Imposes penalties for disclosure of such records.

Establishes the Office of Professional Standards Review in the Department of HEW to administer this Act.

H. R. 3113. Mr. Mosher; 2/10/75. Judiciary, Biester, Boggs, Cohen, Fenwick, Fish, Hechler, Jeffords, McCloskey, Melcher, Miller (Calif.), Mitchell (Md.), Patterson, Rangel, Schroeder, Studds.

See Digest of H. R. 214.

H. R. 3235. Mr. Goldwater; 2/19/75. Judiciary, Badillo, Beard (R. I.), Boland, Carr, Chisholm, Conable, Conyers, D'Amours, Davis, de Lugo, Dellums, Drinan, Duncan (Tenn.), Edgar, Edwards (Calif.) Findley, Fish, Gaydos, Giaimo, Guyer, Harrington, Hicks, Hinshaw, Koch.

See Digest of H. R. 1984.

H. R. 3236. Mr. Goldwater; 2/19/75. Judiciary, Holt, Horton Koch, Lent, Long (Md.), McKinney, Melcher, Miller (Calif.), Mitchell (Md.), Moorhead (Calif.), Murtha, Nix, O'Hara, Obey, Pattison, Rangel, Rees, Richmond, Rinaldo, Roybal, Ryan, Sarasin, Schroeder, Solarz.

See Digest of H. R 1984.

H. R. 3237. Mr. Goldwater; 2/19/75. Judiciary, Koch, Spence Stark, Studds, Traxler, Tsongas, Whitehurst, Wilson (Tex.), Won Pat.

See Digest of H. R. 1984.

H. R. 3284. Mr. Steelman; 2/19/75. Judiciary, Biester, Buchanan, Chisholm, Coughlin, Goldwater, Gude, Hannaford, Harrington, Horton, Leggett, Lent, Matsunaga, Obey, Pattison, Quie, Riegle, Tsongas.

See Digest of H. R. 266.

H. R. 3467. Mr. Mosher; 2/20/75. Judiciary, Baldus, Fauntroy, Howe, Jeffords, Matsunaga, Spellman, Steelman, Stokes.

See Digest of H. R. 214.

H. R. 3655. Mr. Koch; 2/25/75.
Interstate and Foreign Commerce.

Newsmen's Right to Privacy Act - Provides that it shall be unlawful for any telephone company or telegraph company to disclose information with respect to any member of the news media without a court order issued upon the finding that the disclosure of such information (1) will not reveal or threaten to reveal the identity of any source of information with respect to the member of the news media involved in such action; or (2) will serve a compelling and overriding national interest.

Sets forth penalties for violation of the provisions of this Act.

H. R. 3730. Mr. Litton; 2/25/75. Education and Labor, Corman, Hammerschmidt, Jeffords, Roush, Schroeder, Wolff.

See Digest of H. R. 609.

H. R. 3732. Mr. Litton; 2/25/75. Ways and Means, Boland, Burlison, Cotter, Davis, Ford (Tenn.), Forsythe Fulton, Gilman, Hechler, Hinshaw, Krebs, Mezvinsky, Mollohan, Mosher, Nedzi, Roe, Sarbanes, Schroeder, Thompson, Thone, Waggonner Wilson (Tex.), Wilson, Charles H., Won Pat.

See Digest of H. R. 616.

H. R. 3754. Mr. Ashbrook; 2/26/75.
Post Office and Civil Service.

Eliminates the criminal penalties imposed for failure of an individual to answer questions submitted in connection with a census of agriculture, irrigation, or drainage.

(Adds 13 U.S.C 225(e))

H. R. 3855. Mr. Hammerschmidt; 2/27/75. Judiciary.

See Digest of H. R. 214.

H. R. 3874. Mr. Mosher; 2/27/75. Judiciary, Hammerschmidt, Keys, Long (Md.).

See Digest of H. R. 214.

H. R. 4193 Mr. Litton; 3/4/75. Ways and Means, Andrews (N. D.), Archer, Badillo, Bergland, Conyers, Derwinski, Edwards (Calif.), Frenzel, Jones (Okla), Ketchum, Leggett, Lott, McCormack, McKinney, Moorhead (Calif.), Nowak, O'Hara, Ottinger, Rieqle, Seiberling, Stark, Symms, Waxman, Wirth.

See Digest of H. R. 616.

H. R. 4194 Mr. Litton; 3/4/75. Ways and Means, Ashbrook, Bowen, Brown (Calif.), Clay, Collins (Ill.), de Lugo, Dodd, Eckhardt, Eilberg, Fascell, Ginn, Guyer, Holtzman, Jeffords, Koch, Neal, Rangel, Rees, Richmond, Ryan, Santini, Satterfield, Solarz, Yates.

See Digest of H. R. 616.

H. R. 4195. Mr. Litton; 3/4/75. Ways and Means, Abzug, Addabbo, Bedell, Benitez, Bevill, Carr, Coughlin, Dellums, Devine, Evans (Ind.), Fuqua, Gude, Harrington, Kemp, McDonald, Nix, Quie, Rooney, Rose, Rosenthal, Roybal, Studds, Udall, Wolff

See Digest of H. R. 616.

H. R. 4339 Mr. Steelman; 3/5/75. Judiciary, Goldwater, Hammerschmidt, Hawkins, Horton, McCormack.

See Digest of H. R. 266.

H. R. 4433. Mr. Litton; 3/6/75. Ways and Means, Anderson (Ill.), Brodhead, Downey, Drinan, Duncan (Tenn), Helstoski, Keys, Long (Md.), Pressler.

See Digest of H. R. 616.

H. R. 4561. Mrs. Spellman; 3/10/75.
Post Office and Civil Service.

See Digest of H. R. 1674.

H. R. 5045. Mr. Litton; 3/17/75. Ways and Means, Boggs, Daniels, Dominick V., Danielson, Ford (Mich.), Frey, Giaimo, Heckler, Jenrette, McCloskey, Mikva, Murtha, O'Brien, Ruppe, Sisk, Steelman, White.

See Digest of H. R. 616.

H. R. 5128. Ms. Abzug; 3/18/75. Government Operations, Stark, Stokes, Wilson (Tex.), Won Pat.

See Digest of H. R. 2635.

H. R. 5129. Ms. Abzug; 3/18/75. Government Operations, Addabbo, Badillo, Baucus, Boggs, Burke (Calif.) Carr, Danielson, Dellums, Drinan, Edgar, Ford (Tenn.), Hannaford, Harrington, Koch, Maguire, Melcher, Mikva, Mitchell (Md.), Nix, Pattison, Richmond, Roe, Solarz, Spellman.

See Digest of H. R. 2635.

H. R. 5198. Mr. Litton; 3/19/75. Ways and Means, Abdnor, Carney, Hawkins, Lagomarsino, Pritchard, Sarasin.

See Digest of H. R. 616.

H. R. 5324. Mr. Hammerschmidt; 3/21/75. Veterans' Affairs, Teague.

Authorizes the Veterans Administration to release the names and addresses of present or former personnel of the armed services and their dependents to service organizations recognized by law for the preparation, presentation, and prosecution of claims under laws administered by the Veterans' Administration, and to other public or private organizations when the Administrator determines that such release would be in the best interest and overall general welfare of veterans and their dependents. (Amends 38 U.S.C. 3301(9))

H. R. 5410. Mr. Litton; 3/24/75. Ways and Means, Alexander, Bonker, Brown (Mich.), Burke (Calif.), Burton, John L., Cochran, Emery, Fauntroy, Fithian, Hansen, Harkin, Holt, Jones (N. C.), Lloyd (Tenn.), Meeds, Melcher, Mitchell (Md.), Obey, Runnels, Sullivan, Traxler, Wright, Zeferetti.

See Digest of H. R. 616.

H. R. 5437. Mr. Koch; 3/25/75. Judiciary, Schroeder, Solarz Spellman, Stark, Stokes, Waxman, Wilson, Charles H..

See Digest of H. R. 2596.

H. R. 5438. Mr. Koch; 3/25/75. Judiciary, Abzug, Badillo, Baucus, Brown (Calif.), Burton, John L., Burton, Phillip, Carney, Clay, Conyers, Hannaford, Harrington, Holtzman, Meyner, Mikva, Mitchell (Md.), Mottl, Pattison, Rangel, Richmond, Rosenthal, Roybal, Ryan, Scheuer.

See Digest of H. R. 2596.

H. R. 5469. Mr. Litton; 3/25/75. Ways and Means, Bolling, Butler, Fenwick, Flowers, Hamilton, Mann, McHugh, Oberstar, Reuss, Whitehurst.

See Digest of H. R. 616.

H. R. 5515. Mr. Karth; 3/26/75. Ways and Means; Interstate and Foreign Commerce.

Provides, under the Social Security Act, for the establishment and revision of Professional Standards Review Organization areas, such establishment and revision to take into account the recommendations of the doctors of medicine or osteopathy.

States that the final determination in the establishment or revision of any Professional Standards Review Organization area shall be subject to review in a civil action commenced by any interested person.

Directs the National Professional Standards Review Council to conduct a study for the purpose of evaluating whether, and under what conditions, organizations other than professional associations shall be allowed to perform review functions.

Requires each Professional Standards Review Organization to assume responsibility for professional standards review of health care services furnished by or in institutions operated by the Public Health Service and the Veterans Administration in the area which it serves.

Requires, in conjunction with such reviews, that procedures be developed whereby deficiencies shall be brought to the attention of administrators of the hospitals and other Federal institutions concerned. Calls for the consolidation of data and reports compiled under these provisions.

Directs that criteria of health care shall be identified or developed by each Professional Standards Review Organization, giving due consideration to such criteria of care identified or developed by national medical specialty organizations States that such criteria of care shall be used by the Professional Standards Review Organization as guides of care.

Requires the National Professional Standards Review Council to provide for the distribution to each Professional Standards Review Organization, and to each other agency performing review functions, of appropriate materials indicating various guides being utilized in other geographical areas

Provides for the protection of the confidentiality of medical records compiled under this Act.

Empowers the Secretary of Health, Education, and Welfare to enter into a contract with any State medical society or private nonprofit organization (including medical foundations) designated by a State medical society for the provision of necessary technical and other assistance in the creation and operation of local professional standards review organizations.

H. R. 5528. Mr. Martin; 3/26/75. Ways and Means; Interstate and Foreign Commerce.

See Digest of H. R. 5515.

H. R. 5569. Mr. Clausen, Don H.; 3/26/75. Ways and Means.

See Digest of H. R. 616.

H. R. 5597. Mr. Litton; 3/26/75. Ways and Means, Baucus, Blanchard, Cornell, Goodling, Hays, McDonald, Stanton, J. William.

See Digest of H. R. 616.

H. R. 5818. Mr. Litton; 4/9/75. Ways and Means, Aspin, Blouin, Diggs, Madigan, Meyner, Robinson, Roush Simon, Steiger (Wisc.), Weaver.

See Digest of H. R. 616.

H. R. 5819. Mr. Litton; 4/9/75. Ways and Means, Coughlin, Hannaford, Hays, Oberstar, Rangel, Roush, Schroeder, Studds.

See Digest of H. R. 615.

H. R. 5820. Mr. Litton; 4/9/75. Ways and Means, Ford (Tenn.).

See Digest of H. R. 615.

H. R. 6013. Mr. Whalen; 4/15/75. Ways and Means.

See Digest of H. R. 955.

H. R. 6213. Mr. Whalen; 4/21/75. Judiciary.

See Digest of H. R. 215.

H. R. 6390. Mr. Randall; 4/24/75. Ways and Means.

Prohibits the inspection of any Federal income tax return by the Department of Agriculture. Authorizes the Secretary of the Treasury to furnish to the Department of Agriculture, for use only for statistical purposes, the

following data: (1) names and addresses of taxpayers having farming operations; (2) the range of each such taxpayer's gross income from farming operations; and (3) each such taxpayer's type or category of farming operation.

H. R. 6712. Mr. Litton; 5/6/75. Ways and Means, Ashley, Baldus, Breaux, Burke (Mass.), Chappell, Clancy Crane, Dingell, Gaydos, Gradison, Harris, Hicks Kasten, LaFalce, Lent, Martin, Murphy (N. Y.), Patterson, Pike, Risenhoover, Spence, Stokes, Talcott, Vander Jagt.

See Digest of H. R. 616.

H. R. 6713. Mr. Litton; 5/6/75. Ways and Means, Anderson (Calif.), Annunzio, AuCoin, Beard (R. I.), Beard (Tenn), Chisholm, Conable, Daniel, W. C. (Dan), Fraser, Goldwater, Green, Hall, Hubbard, Hughes, Jacobs, Levitas, Lloyd (Calif.), Matsunaga, McClory, McEwen, Metcalfe, Moss, Pattison, Stuckey.

See Digest of H. R. 616.

H. R. 6714 Mr. Litton; 5/6/75. Ways and Means, Esch, Hagedorn, Henderson, Miller (Calif.), Rooney, Spellman, Tsongas.

See Digest of H. R. 616.

H. R. 7234 Mr. Goldwater; 5/21/75. Judiciary, Anderson (Calif.), Blanchard, Cohen, Collins (Ill.), Conte, Coughlin, Downey, Esch, Hannaford, Heinz Kelly, Koch, McCormack, Mezvinsky, Mikva, Moakley, O'Brien, Spellman, Symington.

See Digest of H. R. 1984.

H. R. 7482. Mr. Stark; 5/22/75.
Banking, Currency and Housing, Addabbo, Armstrong, AuCoin, Bedell, Burke (Calif.), Carney, Conlan, Conyers, Danielson, Drinan, Fascell, Fuqua, Gaydos, Giaimo, Harris, Hyde, Jenrette, Kemp, Keys, McKinney, Melcher, Mikva, Miller (Calif.).

See Digest of H. R. 2752.

H. R. 7483 Mr. Stark; 5/22/75.
Banking, Currency and Housing, Ford (Mich.), Jones (Okla.), Obey, Preyer, Richmond, Santini, Scheuer, Seiberling, Steelman, Studds, Weaver, Wilson (Tex.).

See Digest of H. R. 2752.

H. R. 7649. Mr. Stark; 6/5/75.
Banking, Currency and Housing, Abzug, Badillo, Beard (R. I.), Blanchard, Carr, Edgar, Gilman, Howe, Ketchum, Krebs, Lagomarsino, Leggett, Lent, Mann, Martin, McKay, Meyner, Mineta, Murtha, Sarasin, Sarbanes, Solarz, Wirth.

See Digest of H. R. 2752.

H. R. 7781. Mr. Bennett; 6/11/75. Armed Services.

Specifies, under the National Security Act, that the Central Intelligence Agency shall be concerned only with foreign intelligence activities of the United States.

States that the Agency shall inform United States citizens when it is collecting foreign intelligence from them in the United States except when authorized not to make such disclosure by a published Executive Order of the President.

Limits the responsibility of the Agency in protecting sources and methods of foreign intelligence from unauthorized disclosure: (1) to lawful means with respect to present or former employees or contracted agents; and (2) to providing assistance to other governmental intelligence activities.

H. R. 7856. Mr. Steelman; 6/12/75. Judiciary, Railsback.

See Digest of H. R. 266.

H. R. 8227. Mr. Edwards (Calif.); 6/25/75. Judiciary.

Criminal Justice Information Control and Protection of Privacy Act - Title I: Purpose and Scope - Declares it to be the finding of Congress that effective law enforcement requires the dissemination of complete and accurate criminal justice information, but the irresponsible use of inaccurate information may infringe on individual rights. Defines terms used in this Act. Lists the criminal justice agencies to which this Act applies, including: (1) agencies which exchange information interstate; and (2) information obtained from a foreign government or international agency to the extent it is comingled with information obtained from domestic sources. Lists the records and proceedings to which this Act does not apply, including original books of entry or police blotters, and court records of public criminal proceedings.

Title II: Collection and Dissemination of Criminal Justice Information; Criminal Justice Investigative Information; and Criminal Justice Intelligence Information - Prescribes the procedures for: (1) dissemination, access, and use of criminal justice information by criminal justice agencies; (2) dissemination of identification record and wanted persons record information; (3) dissemination, access, and use of criminal justice information by noncriminal justice agencies; and (4) dissemination, access,

and use of criminal justice information with respect to appointments and employment investigations.

Prohibits agencies having access to criminal justice information from disseminating it to others not authorized to have it or from using it for a purpose not authorized by this Act, with limited exceptions with regard to correctional officials.

Requires requests for information to identify the individual to whom the information relates by name except when the information is requested in connection with research related to the administration of criminal justice or in developing investigative leads for a particular offense.

Directs each criminal justice agency to adopt procedures providing: (1) for the security, accuracy, and updating of criminal justice information; and (2) for the sealing and purging of criminal justice information. Provides for access to criminal justice information by an individual or his attorney for purposes of challenging the accuracy, completeness, or legality of such information. Requires criminal justice agencies to adopt rules to implement the granting of such access.

Places limitations on the collection and dissemination of intelligence information. Prohibits direct remote terminal access to criminal justice information except for specified types of information. Enumerates the conditions under which criminal justice investigative information may be disclosed.

Title III: Administrative Provisions; Regulations; Civil Remedies; Criminal Penalties - Establishes the Commission on Criminal Justice Information. States that the Commission shall have overall responsibility for the administration and enforcement of this Act. States that the Commission shall be composed of 13 members, including the Attorney General and nine members appointed by the President with the advice and consent of the Senate. Sets five years as the duration of the Commission

Sets forth the powers and duties of the Commission, including the issuance of such regulations, interpretations and procedures as are necessary to effectuate the provisions of this Act. Authorizes the Commission to conduct hearings, and to exercise subpena powers to insure the presence of witnesses or evidence. Directs the Commission to encourage the formation of State agencies to carry out the provisions of this Act.

Provides judicial remedies to persons aggrieved by a violation of this Act or regulation issued pursuant to this Act. Provides for both injunctive relief and damages of not less than $100 per violation and reasonable attorneys' fees and costs. Directs that any Government employee who willfully violates this Act shall be fined not more than $10,000.

Authorizes the appropriation of such funds as the Congress deems necessary for the purposes of this Act.

H. R. 8248. Mr. Bell; 6/25/75. Government Operations, Beard (R. I.), Burke (Calif.), Chisholm, Collins (Ill.), Conyers, Edwards (Calif.), Fascell, Ford (Tenn.), Harrington, Jeffords, Lent, Long (Md.), Ottinger, Pepper, Richmond, Ryan, Waxman Wilson (Tex.), Wirth.

See Digest of H. R. 7019.

H. R. 8281. Mr. Badillo; 6/26/75. Judiciary.

Special Prosecutor Act - Directs the United States District Court for the District of Columbia, sitting en banc, to appoint a panel of three of its members to select a Special Prosecutor.

Provides for the compensation and staffing of the Office of Special Prosecutor.

States that the Special Prosecutor has exclusive jurisdiction to investigate and to prosecute in the name of the United States: (1) all offenses or allegations of offenses arising out of the conduct of domestic intelligence or counterintelligence activities within the United States by the Central Intelligence Agency or any other law enforcement agency of the Federal Government; (2) all violations or suspected violations of any Federal statute by any intelligence or law enforcement agency of the Federal Government or by any persons on their behalf, such as surreptitious entries, wiretapping, or illegal opening of the United States mail; and (3) such related matters which he consents to have assigned to him by the Attorney General of the United States.

Provides that all files, records, documents, and other materials in the possession or control of the Department of Justice, or any other department or agency of Government, which relate to matters within the exclusive jurisdiction of the Special Prosecutor appointed under this Act, are transferred to the Special Prosecutor as of the date on which he takes office.

Authorizes the Special Prosecutor to request from any department or agency of Government any additional files or other materials which he may deem necessary to the conduct of his duties under this Act.

Stipulates that the Office of Special Prosecutor shall terminate three years after the date the panel first appoints a Special Prosecutor.

Requires the Speical Prosecutor to make as full and complete a report of the activities of his office as is appropriate to the panel, to the Attorney General of the United States, and to the Congress, on the first and second anniversaries of his taking office and not later than thirty days after the termination of the Office of Special Prosecutor.

Grants the panel exclusive jurisdiction to remove the Special Prosecutor.

Authorizes to be appropriated such sums as are necessary to carry out the purposes of this Act.

H. R. 8306 Mr. Rinaldo; 6/26/75.
Banking, Currency and Housing.

See Digest of H. R 2752.

H. R. 8661. Mr. Annunzio; 7/16/75.
Banking, Currency and Housing.

Fair Credit Reporting Act Amendments - Prohibits, under the Fair Credit Reporting Act, a consumer reporting agency from making any consumer report containing records of arrest or criminal conviction if the consumer involved: (1) was sentenced under the Youth Corrections Act; (2) was not convicted of a crime of violence; and (3) subsequently received a certificate setting aside his conviction.

Provides that no consumer reporting agency may make any report containing information of records of arrest or indictment if: (1) the police have elected not to refer a matter to a prosecutor; (2) a prosecutor has elected not to commence criminal proceedings; or (3) a case results in: (a) acquittal, (b) charge dismissed, (c) nolle prosequi, (d) no paper, or (e) case continued without finding.

H. R. 8802. Mr. Melcher; 7/22/75.
Banking, Currency and Housing.

See Digest of H. R. 8661.

H. R. 8806. Mr. Patterson; 7/22/75.
Banking, Currency and Housing.

See Digest of H. R 2752.

H. R. 9002. Mr. Koch; 7/29/75. Judiciary, Carr, Downey, Ford (Tenn.), Tsongas.

See Digest of H. R 564.

H. R. 9165. Mr. Harrington; 7/31/75.
Interstate and Foreign Commerce.

Communications Privacy Act - Prohibits, under the Communications Act of 1934, all disclosures of telephone records except through service of a court subpena meeting specified criteria.

Requires in all cases, except where the telephone subscriber is a foreign power, that the party subpenaing the records notify the subscriber simultaneously that records of his telephone conversations are being subpenaed. Allows such notification to be postponed if the Government satisfies the court that notification would impede an ongoing criminal investigation or would hamper the Government's ability to protect national security interests.

Prohibits the telephone company from responding to such a subpena for at least ten days.

H. R. 9442. Mr. Litton; 9/8/75. Ways and Means, Fisher, Nolan.

See Digest of H. R. 616.

H. R. 9515. Mr. Mezvinsky; 9/10/75. Judiciary.

Bill of Rights Procedures Act - Increases the penalties for illegal warrantless searches by employees of Federal, State, or local governments to a fine of up to $10,000, imprisonment up to 1 year, or both.

Requires court orders for the interception of all forms of communications by electronic and other devices.

Declares that it shall not be unlawful for a person to intercept a wire, oral, or other communication where all parties to the communication have given prior knowing, express, and written permission for such interception.

Requires information concerning intercepted wire, oral, and other communications to be reported to the Administrative Office of the United States Courts and to the Senate and House of Representatives.

Enumerates reporting requirements in the case of warrants sought authorizing the opening of mail.

H. R. 9599. Mr. Vanik; 9/15/75. Ways and Means, Gibbons, Rangel, Stark, Vander Veen.

Federal Taxpayers' Rights Act - Directs the Secretary of the Treasury to prepare pamphlets which set forth in nontechnical terms (1) the rights and obligations of a taxpayer and the Internal Revenue Service during an audit; (2) the procedures by which a taxpayer may appeal any adverse decision of the Service (including administrative and judicial appeals); (3) the procedures for prosecuting refund claims and filing of taxpayer complaints; and (4) the procedures which the Service may use in enforcing the internal revenue laws (including assessment, jeopardy assessment, levy and distraint, and enforcement of liens).

Establishes within the Internal Revenue Service an office to be known as the Office of Taxpayer Services to be under the supervision and direction of an Assistant Commissioner of Internal Revenue who shall assist taxpayers in obtaining easily understandable tax information and answering questions on tax liability, among other functions.

States that, upon application filed by a taxpayer, the Assistant Commissioner for Taxpayer Services may issue a Taxpayer Assistance Order if, in the determination of the Assistant Commissioner, the taxpayer is suffering from an unusual, unnecessary, or irreparable loss as a result of the manner in which the internal revenue laws are being administered by the Secretary or his delegate.

Authorizes the President of the Legal Services Corporation to establish Taxpayer Representation Offices in four cities (selected by the President) for purposes of providing legal assistance to individuals in connection with: (1) any audit by the Service of any return made by or

on behalf of the individual with respect to any tax imposed by chapter 1 of the Internal Revenue Code of 1954, or (2) an assessment or collection from any such individual of any tax imposed by such chapter.

Provides for show cause hearings with respect to jeopardy assessments and termination of taxable years.

Increases the monetary value of specified items to be exempt from levy.

Provides criminal penalties (a fine of up to $10,000, imprisonment for up to 2 years, or both) for investigation into or surveillance over the beliefs, associations, or activities of any individual or organization which are not directly related to such revenue laws. Prohibits a civil cause of action for damages or an injunction, or both, for such violations.

Prohibits inspection of tax returns pursuant to a criminal investigation unless a search warrant has been issued upon probable cause to believe that no alternative source of necessary information is available.

Provides rules for civil investigation related to: (1) payment of Social Security and Railroad Retirement Taxes; (2) pension administration; (3) census information; (4) enforcement of taxpayer's rights under this Act; (5) inspection by States; (6) inspection by a Committee of Congress; and (7) disclosure to persons having a substantial interest (agents of partnerships and corporations, and shareholders of corporations).

Provides a civil action for damages for unauthorized disclosure of tax information.

H. R. 9666. Mr. Harrington; 9/17/75.
Interstate and Foreign Commerce, Abzug, Badillo Brodhead, Chisholm, Clay, Collins (Ill.), Dellums, Edwards (Calif.), Ford (Tenn.), Hannaford, Helstoski, Krebs, McHugh, Mitchell (Md.), Moakley, Moorhead (Pa.), Patterson, Roybal, Stark, Wilson (Tex.).

See Digest of H. R. 9165.

H. R. 9735. Mr. Litton; 9/19/75. Ways and Means.

Taxpayer Privacy Act - Prohibits, generally, disclosure of tax returns or return information by officers or employees of the United States or any State.

Authorizes disclosure of income tax returns to specified persons and entities including: (1) the taxpayer for whom the return was made or his attorney in fact; (2) officers and employees of Federal and State agencies charged with the administration and enforcement of the tax laws; (3) the joint committee on Internal Revenue Taxation; (4) shareholders owning outstanding stock of any corporation, in the case of a return of the corporation; and (5) the President.

Authorizes disclosure to the taxpayer's agent in the case of the taxpayer's death or bankruptcy.

Provides criminal penalties of up to $10,000, imprisonment of up to five years, or both, for unauthorized disclosures by public employees, or unauthorized receipt of tax information by any person from a public employee, under this Act.

Provides an additional criminal penalty of $1,000 for unauthorized disclosure or receipt of a tax return or tax return information by any person.

H. R. 9804. Mr. Anderson (Calif.); 9/24/75. Ways and Means.

See Digest of H. R. 9599.

H. R. 9822. Mr. Vanik; 9/24/75. Ways and Means, Brown (Calif.), Chisholm, Drinan, Edgar, Eilberg, Ford (Tenn.), Harrington, Jenrette, Keys, LaFalce, Long (Md.), Mathis, Meeds, Moakley, Moorhead (Pa.), Rodino, Russo, Sharp, Studds, Thompson, Waxman, Wilson (Tex.), Wirth, Wright.

See Digest of H. R. 9599.

H. R. 9920. Mr. Roush; 9/30/75. Government Operations.

Provides, under the Privacy Act, that individual Members of Congress may receive information from Federal agencies regarding individuals.

H. R. 9925. Mr. Anderson (Calif.); 9/30/75. Government Operations.

Provides, under the Privacy Act, that individual Members of Congress may receive information from Federal agencies regarding individuals.

H. R. 9942. Mr. Ford (Mich.); 10/1/75. Government Operations.

Authorizes, under the Privacy Act of 1974, the disclosure to individual Members of Congress or their designates of information regarding individuals. [Amends 5 U.S.C. 552a]

H. R. 9951. Mr. Perkins; 10/1/75. Government Operations.

Revises the Privacy Act of 1974 to allow the disclosure of information regarding individual constitutents to individual Members of Congress.

H. R. 10002. Mr. Anderson (Calif.); 10/3/75. Government Operations, Bevill, de Lugo, Heinz, Henderson, Hubbard, Hyde, Johnson (Calif.), Ketchum, Mazzoli, Moore, Moorhead (Calif.), Oberstar, Ottinger, Pepper, Rodino, Sebelius, Solarz, Thone, Walsh, Wright, Young (Fla.).

See Digest of H. R. 9925.

H. R. 10023. Mr. Roush; 10/3/75. Government Operations, Broyhill, Byron, Conte, Daniel, W. C. (Dan), Eshleman, Fish, Ginn, Goodling, Hechler, Johnson (Calif.), Lehman, Pepper, Pike, Quie, Scheuer, Sharp, Simon, Wampler, Whitehurst.

See Digest of H. R. 9920.

H. R. 10050. Mr. Waggonner; 10/6/75. Government Operations.

See Digest of H. R. 9925.

H. R. 10134. Mr. Ford (Mich.); 10/9/75. Government Operations, Ashbrook, Bedell, Bevill, Boland, Brown (Mich.), Burlison, Conyers, Derwinski, Devine, Diggs, duPont, Eilberg, Emery, Esch, Evins, Gibbons, Gonzalez

See Digest of H. R. 9942.

H. R. 10135. Mr. Ford (Mich.); 10/9/75. Government Operations, Harris, Hawkins, Hechler, Helstoski, Howe, Hughes, Ichord, Jeffords, Johnson (Calif.), Jordan, LaFalce, Lent, Long (Md.), Maguire, Mazzoli, McKinney, Meeds.

See Digest of H. R. 9942.

H. R. 10136. Mr. Ford (Mich.); 10/9/75. Government Operations, Melcher, Nix, Patterson Pattison, Pepper, Railsback, Rostenkowski, Shipley, Simon, Solarz, Stratton, Thompson, Van Deerlin, Vander Veen, Vigorito, Waxman, White, Yatron.

See Digest of H. R. 9942.

H. R. 10159. Mr. Anderson (Calif.); 10/9/75. Government Operations, Boland, Burgener, Heckler, Lloyd (Calif.), McCormack, Pattison, Pettis, Shirley N., Waxman, Wilson (Tex.).

See Digest of H. R. 9925.

H. R. 10368. Mr. Anderson (Calif.); 10/28/75. Government Operations, Cochran, Holt, Johnson (Pa.), Spellman.

See Digest of H. R. 9925.

H. R. 10387. Mr. Matsunaga; 10/28/75. Ways and Means.

See Digest of H. R. 9599.

H. R. 10425. Mr. Mosher; 10/29/75. Judiciary, Hawkins, Maguire.

See Digest of H. R. 214.

H. R. 10450. Mrs. Spellman; 10/30/75. Government Operations.

See Digest of H. R. 9942.

H. R. 10960. Mr. Vanik; 12/2/75. Ways and Means, Anderson (Calif.), Baucus, Downey, Fraser, Harris, Hawkins, Heckler, Mikva, Moakley, Moffett, Neal, Ottinger, Pattison, Rosenthal, Ryan, Santini, Schroeder, Seiberling, Spellman, Weaver.

See Digest of H. R. 9599.

H. R. 11090. Mr. Schneebeli (by req.); 12/10/75. Ways and Means.

States that income tax returns and return information shall be confidential. Defines returns and return information for purposes of this Act.

Permits the inspection of returns and return information by individuals filing such returns, by State tax officials, corporation officials, trustees, estate administrators, and by the House Ways and Committee, the Senate Finance Committee, and the Joint Committee on Internal Revenue Taxation upon request and in closed session.

Permits the inspection by other committees if authorized by resolution. Allows the inspection of returns and return information by the President on his written request personally signed by him, or returns and return information by the President or his designees by name upon his order, and by Justice Department attorneys, without request, for use in relevant proceedings under the tax laws.

Allows such inspection, under specified conditions, by the Commerce Department for statistical purposes and by other executive officials for administrative or judicial proceedings other than under the tax laws.

Conditions the foregoing inspections upon whether: (1) the taxpayer is a party to the proceedings; (2) the taxpayer consents; or (3) such return information has or may have a bearing on the outcome of such proceedings.

Allows limited inspection of return information by authorized executive officials for purposes of assessing persons being considered for appointments to the judicial or executive branch of the Government.

Authorizes the disclosure of return information to the Attorney General when such information indicates possible criminal violations.

Sets forth procedures for disclosure and inspection of return information, including maintenance of a record of who inspects such return.

Establishes penalties for unauthorized disclosure of return information.

H. R. 11105. Mr. Crane; 12/11/75.
Interstate and Foreign Commerce.

Prohibits government officials from examining the medical or dental records of persons who are not receiving medical care paid for in whole or in part by the Federal Government.

H. R. 11129. Mr. Kastenmeier; 12/11/75. Judiciary.

Extends for three months the authority, under the Omnibus Crime Control and Safe Streets Act, of the National Commission for the Review of Federal and State Laws relating to wiretapping and electronic surveillance Permits dissenting or additional views to the Commission's final report to be submitted.

H. R. 11307. Mr. Rinaldo; 12/19/75. Ways and Means.

See Digest of H. R. 616.

H. R. 11337. Mrs. Schroeder; 12/19/75.
Post Office and Civil Service, Hinshaw, Lehman Spellman.

Authorizes the Secretary of Commerce to furnish, upon written request, authenticated copies of census surveys or reports filed by, or on behalf of, an individual or organization to such individual or organization or to the heir or agent of such individual or organization.

Allows the Secretary to furnish copies of tabulations and other statistical materials which do not disclose the information reported by any individual or organization to any private person or agency requesting such information upon payment of the cost of such work.

Directs that in no case shall information furnished pursuant to this Act be used to the detriment of any respondent person to whom such information relates.

Directs the Secretary, in the year 1985 and every ten years thereafter, to conduct a mid-decade sample survey of population.

Requires that information obtained in such a survey be used in the determination of eligibility of States, local governments, and other recipients for Federal benefits, if such surveys yield appropriate information.

Stipulates that information obtained in such mid-decade sample surveys shall not be used for apportionment of Representatives in Congress among the several States, nor for prescribing congressional districts.

Requires the Secretary to submit to the Congress the questions proposed to be included in the decennial census and the mid-decade sample survey of population.

Authorizes the Secretary to conduct special censuses for

the government of any State or any political subdivision within a State upon payment to the Secretary of the cost of such special census.

Increases the penalty for wrongful disclosure of census information by census employees from a fine of $1,000 and two years imprisonment to a fine of $5,000 and five years imprisonment.

Repeals the provisions for penalties for refusal to answer questions. Removes the imprisonment penalty (retaining the fine) for making false answers to a census questionnaire.

Provides that if a provision enacted by this Act is held invalid, all valid provisions that are severable from the invalid provision shall remain in effect.

Effectuates this Act on October 1, 1976, or the date of enactment, whichever is later.

3-24-76	Reported to House from the Comm. on Post Office and Civil Service with amendment, H. Rept. 94-944
4-07-76	Measure called up by special rule in House
4-07-76	Measure considered in House
4-07-76	Measure passed House, amended
4-08-76	Referred to Senate Committee on Post Office and Civil Service

H. R. 11511. Mr. Crane; 1/27/76.
Interstate and Foreign Commerce, Carter, Davis Derwinski, Grassley, Kelly, Ketchum, Martin, McDonald.

Prohibits the inspection, acquisition, or requisition by officers, employees, agents or departments of the United States of the medical or dental records of patients not receiving assistance from the Federal Government.

Imposes penalties for violation of this Act.

H. R. 11780. Mr. Litton; 2/9/76. Ways and Means, Cochran.

States that all returns made with respect to the taxes imposed by the Internal Revenue Code are confidential records. Provides that: (1) no such return shall be open to inspection; and (2) no information contained in any such return shall be disclosed.

Authorizes inspections by the following persons: (1) the taxpayer or his authorized representative; (2) officers and employees of the Internal Revenue Service, Department of the Treasury, Department of Justice, and State and local government employees solely for purposes of enforcement and administration of the tax laws; and (3) the President of the United States in the necessary performance of his official duties.

Increases the criminal penalties for unauthorized disclosure of information under the provisions of the Internal Revenue Code.

States that any person who knowingly receives any information or material which is disclosed or furnished in

violation of the provisions of this Act shall be guilty of a felony and subject to a fine of up to $10,000, imprisoned for up to five years, or both.

H. R. 11896. Mr. Crane; 2/17/76.
Interstate and Foreign Commerce, Goldwater, Robinson.

See Digest of H. R. 11511.

H. R. 11953. Mr. Steiger (Wisc.); 2/18/76. Ways and Means.

Establishes conditions, under the Internal Revenue Code, which the State agency, body, or commission lawfully charged with tax administration must meet before the Secretary of the Treasury shall allow the inspection or disclosure of income tax returns or return information.

Requires the written request of the head of such State agency, body, or commission before such return information shall be furnished.

H. R. 12039. Ms. Abzug; 2/24/76. Government Operations.

Amends the Privacy Act of 1974 with respect to records maintained on individuals to require Federal agencies to correct, expunge, update, or supplement portions of records on any individual upon request by such individual. Requires such agency to inform each person (1) whose correspondence has been intercepted or examined, (2) who is the subject of a file of CHAOS, COINTELPRO, or "The Special Service Staff" of the Internal Revenue Service, or (3) who is named in an index of such organizations, that such records exist; to inform each person of such person's rights under the Privacy Act of 1974; and to permit such person to require destruction of such file or index.

H. R. 12624. Mr. Crane; 3/18/76.
Interstate and Foreign Commerce, Bafalis, Burgener, Collins (Tex.), Conlan, Fauntroy, Harrington, Kemp, Martin, Melcher, Rose, Whitehurst, Wilson, Charles H., Won Pat.

See Digest of H. R. 11511.

H. R. 12750. Mr. Rodino; 3/23/76. Judiciary, Danielson, Hutchinson, Kastenmeier, Mosher, Pattison, Railsback, Wiggins.

Foreign Intelligence Surveillance Act - Requires the Chief Justice of the United States to designate seven district court judges, each of whom shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States. Requires the Chief Justice to designate three Federal judges to comprise a special court of appeals which shall have jurisdiction to hear an appeal by the United States from the

denial of any application. Grants the United States a further right to appeal an affirmance of denial to the Supreme Court.

Requires each application for any order approving electronic surveillance for foreign intelligence purposes to be approved by the Attorney General and to include: (1) the identity of the officer making the application; (2) the authority conferred on the applicant by the President and the approval of the Attorney General to make the application; (3) the identity of the subject of the surveillance; (4) the fact and circumstances justifying belief that the target of surveillance is a foreign power or an agent of a foreign power; (5) a description of the type of information sought and a certification by one of specified Federal officers that such information is foreign intelligence information that cannot feasibly be obtained by normal investigative techniques; and (6) a statement of the period of time for which the surveillance is required.

Directs the judge to enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that the criteria specified have been met. Allows issuance of orders to approve surveillance for 90 days or the period necessary to achieve its purposes, whichever is less. Permits extensions of orders upon application for an extension made in the same manner as required for an original application.

Authorizes the Attorney General, upon a reasonable determination that an emergency situation exists, to authorize the emergency employment of electronic surveillance if an appropriate judge is informed by the Attorney General of such authorization at the time it is made and if an application is made as soon as practicable but not more than 24 hours after authorization. Requires, in the absence of a judicial order, that surveillance terminate when the information sought is obtained, when the application for an order is denied, or 24 hours after authorization, whichever is earliest.

Allows information acquired from electronic surveillance conducted pursuant to this Act to be used and disclosed only for designated purposes or for the enforcement of the criminal law.

Requires when an order to approve the emergency employment of electronic surveillance is not obtained, that the judge serve notice on the individual subject to surveillance of the fact of the application, the period of surveillance, and the fact that information was or was not obtained. Permits the judge to delay or forego this action on a showing of good cause.

Requires the Attorney General to submit an annual report to the Administrative Office of the United States Courts and to Congress including: (1) the number of applications made for orders and extensions of orders approving electronic surveillance and the number of such orders and extensions granted, modified, and denied; (2) the periods of time for which orders authorized surveillances and their actual duration; (3) the number of surveillances in place at any

time during the preceding year; and (4) the number of surveillances terminated during the preceding year.

Declares that nothing contained in this Act shall limit the Constitutional power of the President to order electronic surveillances for specified national security reasons if the facts and circumstances giving rise to such order are beyond the scope of this Act. [Amends 18 U.S.C. 2521-2528]

H. R. 13120. Mr. Devine; 4/8/76. Judiciary.

See Digest of H. R. 12750.

H. R. 13191. Ms. Abzug; 4/13/76. Judiciary.

Makes it a crime for any Federal officer or employee or a person engaged in any activity in or affecting interstate commerce, or anyone acting under the authority of such individuals, to permit, require, or request anyone applying for employment to take a polygraph test in connection with employment duties or services, or in connection with such person's application for employmnet. Makes it a crime to deny employment to any individual, or to discharge, discipline, or deny promotion, or to threaten to commit any such act by reason of such individual's refusal or failure to submit to a polygraph test. Subjects violators to a fine not exceeding $1,000.

Stipulates that whenever these provisions are violated, any affected person may bring a civil action against the officer in the appropriate United States district courts. Grants the district courts of the United States jurisdiction over such actions regardless of the actuality or amount of pecuniary injury done or threateded, and without regard to whether the aggrieved party has exhausted administrative remedies. Empowers such courts to issue restraining orders, interlocutory injunctions, permanent injunctions, or mandatory injunctions, or to enter such other judgments or decrees as are necessary or appropriate to prevent the threatened violation or afford the plaintiff and other similarly situated individuals complete relief against the consequences of the violation. Permits employee organizations to bring civil actions in such cases on behalf of an aggrieved individual if such individual gives written consent. [Adds 18 U.S.C. 246]

H. R. 13192. Ms. Abzug; 4/13/76. Government Operations, Clay, Conyers, Drinan, Harrington, Helstoski, Koch, Maguire, Mitchell (N. Y.), Moffett, Richmond, Rosenthal, Roybal, Scheuer, Stark, Wilson, Charles H..

See Digest of H. R. 12039.

H. R. 13197. Mr. Cederberg; 4/13/76. Judiciary.

See Digest of H. R. 12750.

H. R. 13376. Mr. Rodino; 4/28/76. Judiciary, Andrews (N. D.), Broyhill, Carter, Downey, Duncan (Ore.), Frenzel, Hannaford, Hughes, Hungate, Hyde, Kemp, Mazzoli, Melcher, Mineta, Patterson, Pike, Sisk, Tsongas, Won Pat.

See Digest of H. R. 12750.

H. R. 13602. Mr. Beard (Tenn.); 5/6/76. Judiciary.

Prescribes penalties for the unauthorized disclosure of classified information. Enumerates defenses available to an individual charged with such offense, including: (1) prior official disclosure; (2) unlawful classification and the exhaustion of available declassification procedures; and (3) the absence of a process for reviewing the continuing necessity for the classification. [Adds 18 U.S.C. 800]

H. R. 13605. Mr. Clausen, Don H.; 5/6/76. Judiciary.

See Digest of H. R. 12750.

H. R. 13681. Ms. Abzug (by req.); 5/11/76. Government Operations.

Deletes the $750,000 per-fiscal-year limitation on the expenditure of appropriations authorized for the use of the Privacy Protection Study Commission established by the Privacy Act of 1974.

H. R. 13682. Ms. Abzug (by req.); 5/11/76. Government Operations.

Changes the authorization for appropriations for the Privacy Protection Study Commission under the Privacy Act of 1974 from $1,500,000 for fiscal years 1975, 1976 and 1977, to $2,000,000 for the period July 1, 1975 through September 30, 1977. Deletes the annual expenditure limitation on such authorization.

H. R. 13757. Mr. Conlan; 5/12/76. Banking, Currency and Housing.

Right to Financial Privacy Act - Prohibits any financial institution from disclosing to a Federal agency any financial record of a customer unless such customer has so authorized or a valid warrant, subpena or summons has been obtained according to the terms of this Act. Provides civil and criminal penalties for violations of this Act, in addition to injunctive relief.

H. R. 14284. Mr. Mosher; 6/9/76. Judiciary, Kemp, Koch.

Bill of Rights Procedures Act - Title I: Confidentiality of Financial, Toll, and Credit Records - Prohibits any United States entity or representative from obtaining copies

of, or access to, information contained in the financial records, toll records, or credit records of any customer of a financial institution, communication common carrier, credit card issuer, or consumer reporting agency. Removes such prohibition if the records are described with sufficient particularity, if the customer has authorized disclosure, and if disclosure is obtained in response to an administrative supoena, search warrant, or judicial subpoena.

Sets forth procedures for obtaining customer authorization, administrative subpoenas and summons, search warrants, and judicial subpoenas.

Requires financial institutions, communication common carriers, credit card issuers, and consumer reporting agencies to keep records of all examinations of customer records, including the identity of the person examining such records, the governmental agency or department such person represents, and a copy of the authorization.

Stipulates that any action under this title may be brought in any appropriate U.S. district court without regard to the amount in controversy, or in any other court of competent jurisdiction, within three years from the date on which the violation occurs or the date of discovery of such violation, whichever is later.

Imposes liability on any person or entity who knowingly obtains or discloses information in violation of this title, making such person or entity liable to the customer to whom the disclosed information relates for actual damages, such punitive damages as the court may allow if the violation was willful, and the costs of litigation. Makes injunctive relief available to any person aggrieved by a violation or threatened violation of this Act.

Title II: Mail Covers - Defines a "mail cover" as the procedures initiated at the request of a law enforcement authority by which a systematic inspection is made of any data appearing on the outside cover of any mail matter.

Prohibits the initiation of any mail cover without the written authorization of specified postal officials and good cause to believe, on the basis of an affidavit setting forth the specific reasons for the proposed mail cover, that such procedure is necessary to the investigation of commission or attempted commission of a felony or is necessary to aid in locating a fugitive.

Permits a mail cover to be conducted for 30 days with extensions to be granted as specified. Requires any mail cover conducted for more than one year to be judicially authorized. Allows the chief postal inspector or a regional chief postal inspector to issue an emergency authorization for a mail cover on the basis of an oral request from specified law enforcement officials, if such request is supported by an affidavit within 45 days and on condition that no data from such mail cover be made available to the requesting authority until authorization according to regular procedures has been granted.

Stipulates that the subjects of mail covers shall be given notice of such cover within 90 days of its

termination, unless notice is judicially waived due to possible jeopardizing of continuing investigations.

Requires that the chief postal inspector submit to Congress an annual report including the number of requests for mail covers, the identity of the law enforcement agencies making such requests, and a list of the offenses for which mail cover requests were received.

Title III: Amendments to Chapter 119, Title 18, United States Code - Sets forth procedures and restrictions governing the interception of wire or oral communications for purposes of supervisory observing or service by communication common carriers and others. Requires each communication common carrier to submit an annual report to the Federal Communications Commission detailing the interceptions made by it for the protection of its service against theft of service, the nature and frequency of communications intercepted, the number of persons whose communications were intercepted, the length of such interceptions, and the number of hours of recording of intercepted communications.

Prohibits the manufacture, distribution, possession, and advertising of devices for theft of communication common carrier services. Stipulates that any such device may be seized and forfeited to the United States.

Title IV: Penalties - Subjects officers, agents, or employees of the United States who violate any provision of title I or title II of this Act to a fine of not more than $1,000, imprisonment for not more than one year, or both.

Title V: Congressional Subpoenas - Stipulates that nothing in this Act shall apply to Congressional subpoenas.

79-064 O - 76 - 52

BILLS AND RESOLUTIONS - 94th CONGRESS

HOUSE RESOLUTIONS

H. Res. 1037 Mr. Badillo; 2/18/76. Judiciary.

Expresses the disapproval of the House of Representatives of the proposed guidelines for domestic intelligence investigations proposed by the Attorney General.

APPENDIX B

Public Law 93-579
93rd Congress, S. 3418
December 31, 1974

An Act

To amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Privacy Act of 1974". Privacy Act of 1974. 5 USC 552a note.

SEC. 2. (a) The Congress finds that— Congressional findings. 5 USC 552a note.

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to— Statement of purpose.

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

88 STAT. 1896
88 STAT. 1897

SEC. 3. Title 5, United States Code, is amended by adding after section 552 the following new section:

5 USC 552a. **"§ 552a. Records maintained on individuals**

"(a) DEFINITIONS.—For purposes of this section—

"(1) the term 'agency' means agency as defined in section 552(e) of this title; 5 USC 552.

"(2) the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence;

"(3) the term 'maintain' includes maintain, collect, use, or disseminate;

"(4) the term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

"(5) the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

"(6) the term 'statistical record' means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13; and 13 USC 8.

"(7) the term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

"(b) CONDITIONS OF DISCLOSURE.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

"(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

"(2) required under section 552 of this title;

"(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

"(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

"(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

"(6) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

"(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which

maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

"(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

"(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

"(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office; or

"(11) pursuant to the order of a court of competent jurisdiction.

"(c) Accounting of Certain Disclosures.—Each agency, with respect to each system of records under its control, shall—

"(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of—

"(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

"(B) the name and address of the person or agency to whom the disclosure is made;

"(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

"(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

"(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

"(d) Access to Records.—Each agency that maintains a system of records shall—

"(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence; Personal review.

"(2) permit the individual to request amendment of a record pertaining to him and— Amendment request.

"(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

"(B) promptly, either—

"(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason

for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

Review.

"(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

Notation of dispute.

"(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

"(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

"(e) AGENCY REQUIREMENTS.—Each agency that maintains a system of records shall—

"(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

"(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

"(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

"(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

"(B) the principal purpose or purposes for which the information is intended to be used;

"(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

"(D) the effects on him, if any, of not providing all or any part of the requested information;

Publication in Federal Register.

"(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include—

"(A) the name and location of the system;

"(B) the categories of individuals on whom records are maintained in the system;

"(C) the categories of records maintained in the system;

"(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

"(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

"(F) the title and business address of the agency official who is responsible for the system of records;

"(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

"(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

"(I) the categories of sources of records in the system;

"(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

"(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

"(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

"(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

"(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance; Rules of conduct.

"(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; and Confidentiality of records.

"(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency. Publication in Federal Register.

"(f) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall— 5 USC 553.

"(1) establish procedures whereby an individual can be notified

in response to his request if any system of records named by the individual contains a record pertaining to him;

"(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

"(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

"(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

Fees. "(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

Publication in Federal Register. The Office of the Federal Register shall annually compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

"(g)(1) CIVIL REMEDIES.—Whenever any agency

"(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

"(B) refuses to comply with an individual request under subsection (d)(1) of this section;

"(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

"(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

Jurisdiction. the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

Amendment of record. "(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

Injunction. "(3)(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of

any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

"(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of— Damages.

"(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

"(B) the costs of the action together with reasonable attorney fees as determined by the court.

"(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to the effective date of this section.

"(h) Rights of Legal Guardians.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

"(i)(1) Criminal Penalties.—Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

"(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

"(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

"(j) General Exemptions.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553 (b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through 5 USC 553.

(F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is—

"(1) maintained by the Central Intelligence Agency; or

"(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section. 5 USC 553.

"(k) SPECIFIC EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4) (G), (H), and (I) and (f) of this section if the system of records is—

5 USC 552. "(1) subject to the provisions of section 552(b)(1) of this title;

"(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: *Provided, however*, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18; 18 USC 3056.

"(4) required by statute to be maintained and used solely as statistical records;

"(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the

Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

"(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553 (c) of this title, the reasons why the system of records is to be exempted from a provision of this section. 5 USC 553.

"(l)(1) Archival Records.—Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section. 44 USC 3103.

"(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register. Publication in Federal Register.

"(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

"(m) Government Contractors.—When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

"(n) Mailing Lists.—An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

"(o) Report on New Systems.—Each agency shall provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records in order to permit an evaluation of the probable or potential effect of such Notice to Congress and OMB.

proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers.

Report to Speaker of the House and President of the Senate.

"(p) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section.

5 USC 552.

(q) EFFECT OF OTHER LAWS.—No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.".

5 USC prec. 500.

SEC. 4. The chapter analysis of chapter 5 of title 5, United States Code, is amended by inserting:

"552a. Records about individuals."

immediately below:

"552. Public information; agency rules, opinions, orders, and proceedings.".

Privacy Protection Study Commission. Establishment. 5 USC 552a note.

SEC. 5. (a)(1) There is established a Privacy Protection Study Commission (hereinafter referred to as the "Commission") which shall be composed of seven members as follows:

Membership.

(A) three appointed by the President of the United States,

(B) two appointed by the President of the Senate, and

(C) two appointed by the Speaker of the House of Representatives.

Members of the Commission shall be chosen from among persons who, by reason of their knowledge and expertise in any of the following areas—civil rights and liberties, law, social sciences, computer technology, business, records management, and State and local government—are well qualified for service on the Commission.

(2) The members of the Commission shall elect a Chairman from among themselves.

Vacancies.

(3) Any vacancy in the membership of the Commission, as long as there are four members in office, shall not impair the power of the Commission but shall be filled in the same manner in which the original appointment was made.

(4) A quorum of the Commission shall consist of a majority of the members, except that the Commission may establish a lower number as a quorum for the purpose of taking testimony. The Commission is authorized to establish such committees and delegate such authority to them as may be necessary to carry out its functions. Each member of the Commission, including the Chairman, shall have equal responsibility and authority in all decisions and actions of the Commission, shall have full access to all information necessary to the performance of their functions, and shall have one vote. Action of the Commission shall be determined by a majority vote of the members present. The Chairman (or a member designated by the Chairman to be acting Chairman) shall be the official spokesman of the Commission in its relations with the Congress, Government agencies, other persons, and the public, and, on behalf of the Commission, shall see to the faithful execution of the administrative policies and decisions of the Commission, and shall report thereon to the Congress from time to time or as the Commission may direct.

(5) (A) Whenever the Commission submits any budget estimate or request to the President or the Office of Management and Budget, it shall concurrently transmit a copy of that request to Congress. Budget requests.

(B) Whenever the Commission submits any legislative recommendations, or testimony, or comments on legislation to the President or Office of Management and Budget, it shall concurrently transmit a copy thereof to the Congress. No officer or agency of the United States shall have any authority to require the Commission to submit its legislative recommendations, or testimony, or comments on legislation, to any officer or agency of the United States for approval, comments, or review, prior to the submission of such recommendations, testimony, or comments to the Congress. Legislative recommendations.

(b) The Commission shall—

(1) make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information; and Study.

(2) recommend to the President and the Congress the extent, if any, to which the requirements and principles of section 552a of title 5, United States Code, should be applied to the information practices of those organizations by legislation, administrative action, or voluntary adoption of such requirements and principles, and report on such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information. Ante, p. 1897.

(c) (1) In the course of conducting the study required under subsection (b) (1) of this section, and in its reports thereon, the Commission may research, examine, and analyze—

(A) interstate transfer of information about individuals that is undertaken through manual files or by computer or other electronic or telecommunications means;

(B) data banks and information programs and systems the operation of which significantly or substantially affect the enjoyment of the privacy and other personal and property rights of individuals;

(C) the use of social security numbers, license plate numbers, universal identifiers, and other symbols to identify individuals in data banks and to gain access to, integrate, or centralize information systems and files; and

(D) the matching and analysis of statistical data, such as Federal census data, with other sources of personal data, such as automobile registries and telephone directories, in order to reconstruct individual responses to statistical questionnaires for commercial or other purposes, in a way which results in a violation of the implied or explicitly recognized confidentiality of such information.

(2) (A) The Commission may include in its examination personal information activities in the following areas: medical; insurance; education; employment and personnel; credit, banking and financial institutions; credit bureaus; the commercial reporting industry; cable television and other telecommunications media; travel, hotel and entertainment reservations; and electronic check processing.

(B) The Commission shall include in its examination a study of—

(i) whether a person engaged in interstate commerce who maintains a mailing list should be required to remove an individual's name and address from such list upon request of that individual;

(ii) whether the Internal Revenue Service should be prohibited from transfering individually indentifiable data to other agencies and to agencies of State governments;

(iii) whether the Federal Government should be liable for general damages incurred by an individual as the result of a willful or intentional violation of the provisions of sections 552a (g) (1) (C) or (D) of title 5, United States Code; and

Ante, p. 1897.

(iv) whether and how the standards for security and confidentiality of records required under section 552a (e) (10) of such title should be applied when a record is disclosed to a person other than an agency.

Religious organizations, exception.

(C) The Commission may study such other personal information activities necessary to carry out the congressional policy embodied in this Act, except that the Commission shall not investigate information systems maintained by religious organizations.

Guidelines for study.

(3) In conducting such study, the Commission shall—

(A) determine what laws, Executive orders, regulations, directives, and judicial decisions govern the activities under study and the extent to which they are consistent with the rights of privacy, due process of law, and other guarantees in the Constitution;

(B) determine to what extent governmental and private information systems affect Federal-State relations or the principle of separation of powers;

(C) examine the standards and criteria governing programs, policies, and practices relating to the collection, soliciting, processing, use, access, integration, dissemination, and transmission of personal information; and

(D) to the maximum extent practicable, collect and utilize findings, reports, studies, hearing transcripts, and recommendations of governmental, legislative and private bodies, institutions, organizations, and individuals which pertain to the problems under study by the Commission.

(d) In addition to its other functions the Commission may—

(1) request assistance of the heads of appropriate departments, agencies, and instrumentalities of the Federal Government, of State and local governments, and other persons in carrying out its functions under this Act;

(2) upon request, assist Federal agencies in complying with the requirements of section 552a of title 5, United States Code;

(3) determine what specific categories of information, the collection of which would violate an individual's right of privacy, should be prohibited by statute from collection by Federal agencies; and

(4) upon request, prepare model legislation for use by State and local governments in establishing procedures for handling, maintaining, and disseminating personal information at the State and local level and provide such technical assistance to State and local governments as they may require in the preparation and implementation of such legislation.

(e) (1) The Commission may, in carrying out its functions under this section, conduct such inspections, sit and act at such times and places, hold such hearings, take such testimony, require by subpena the attendance of such witnesses and the production of such books, records, papers, correspondence, and documents, administer such oaths, have such printing and binding done, and make such expenditures as the Commission deems advisable. A subpena shall be issued only upon an affirmative vote of a majority of all members of the Com-

mission. Subpenas shall be issued under the signature of the Chairman or any member of the Commission designated by the Chairman and shall be served by any person designated by the Chairman or any such member. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission.

(2)(A) Each department, agency, and instrumentality of the executive branch of the Government is authorized to furnish to the Commission, upon request made by the Chairman, such information, data, reports and such other assistance as the Commission deems necessary to carry out its functions under this section. Whenever the head of any such department, agency, or instrumentality submits a report pursuant to section 552a (o) of title 5, United States Code, a copy of such report shall be transmitted to the Commission.

Reports, transmittal to Commission.
Ante, p. 1897.

(B) In carrying out its functions and exercising its powers under this section, the Commission may accept from any such department, agency, independent instrumentality, or other person any individually indentifiable data if such data is necessary to carry out such powers and functions. In any case in which the Commission accepts any such information, it shall assure that the information is used only for the purpose for which it is provided, and upon completion of that purpose such information shall be destroyed or returned to such department, agency, independent instrumentality, or person from which it is obtained, as appropriate.

(3) The Commission shall have the power to——

(A) appoint and fix the compensation of an executive director, and such additional staff personnel as may be necessary, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, but at rates not in excess of the maximum rate for GS–18 of the General Schedule under section 5332 of such title; and

5 USC 5101, 5331.

5 USC 5332 note.

(B) procure temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code.

The Commission may delegate any of its functions to such personnel of the Commission as the Commission may designate and may authorize such successive redelegations of such functions as it may deem desirable.

(4) The Commission is authorized—

(A) to adopt, amend, and repeal rules and regulations governing the manner of its operations, organization, and personnel;

Rules and regulations.

(B) to enter into contracts or other arrangements or modifications thereof, with any government, any department, agency, or independent instrumentality of the United States, or with any person, firm, association, or corporation, and such contracts or other arrangements, or modifications thereof, may be entered into without legal consideration, without performance or other bonds, and without regard to section 3709 of the Revised Statutes, as amended (41 U.S.C. 5);

(C) to make advance, progress, and other payments which the Commission deems necessary under this Act without regard to the provisions of section 3648 of the Revised Statutes, as amended (31 U.S.C. 529); and

(D) to take such other action as may be necessary to carry out its functions under this section.

Compensation.

(f)(1) Each [the] member of the Commission who is an officer or employee of the United States shall serve without additional compensation, but shall continue to receive the salary of his regular position when engaged in the performance of the duties vested in the Commission.

Per diem.

5 USC 5332 note.

(2) A member of the Commission other than one to whom paragraph (1) applies shall receive per diem at the maximum daily rate for GS-18 of the General Schedule when engaged in the actual performance of the duties vested in the Commission.

Travel expenses.

(3) All members of the Commission shall be reimbursed for travel, subsistence, and other necessary expenses incurred by them in the performance of the duties vested in the Commission.

Report to President and Congress.

(g) The Commission shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this section. The Commission shall make a final report to the President and to the Congress on its findings pursuant to the study required to be made under subsection (b)(1) of this section not later than two years from the date on which all of the members of the Commission are appointed. The Commission shall cease to exist thirty days after the date on which its final report is submitted to the President and the Congress.

Penalties.

(h)(1) Any member, officer, or employee of the Commission, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from the Commission under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

5 USC 552a note.

SEC. 6. The Office of Management and Budget shall—

(1) develop guidelines and regulations for the use of agencies in implementing the provisions of section 552a of title 5, United States Code, as added by section 3 of this Act; and

Ante, p. 1897.

(2) provide continuing assistance to and oversight of the implementation of the provisions of such section by agencies.

5 USC 552a note.

SEC. 7. (a)(1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

(2) the provisions of paragraph (1) of this subsection shall not apply with respect to—

(A) any disclosure which is required by Federal statute, or

(B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

SEC. 8. The provisions of this Act shall be effective on and after the date of enactment, except that the amendments made by sections 3 and 4 shall become effective 270 days following the day on which this Act is enacted. Effective date. 5 USC 552a note.

SEC. 9. There is authorized to be appropriated to carry out the provisions of section 5 of this Act for fiscal years 1975, 1976, and 1977 the sum of $1,500,000, except that not more than $750,000 may be expended during any such fiscal year. Appropriation. 5 USC 552a note.

Approved December 31, 1974.

LEGISLATIVE HISTORY:

HOUSE REPORT No. 93-1416 accompanying H.R. 16373 (Comm. on Government Operations).
SENATE REPORT No. 93-1183 (Comm. on Government Operations).
CONGRESSIONAL RECORD, Vol. 120 (1974):
Nov. 21, considered and passed Senate.
Dec. 11, considered and passed House, amended, in lieu of H.R. 16373.
Dec. 17, Senate concurred in House amendment with amendments.
Dec. 18, House concurred in Senate amendments.
WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 11, No. 1:
Jan. 1, Presidential statement.

79-064 O - 76 - 53

Appendix C

United States Code

Chapter 119.—WIRE INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec.
2510. Definitions.
2511. Interception and disclosure of wire or oral communications prohibited.
2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited.
2513. Confiscation of wire or oral communication intercepting devices.
2515. Prohibition of use as evidence of intercepted wire or oral communications.
2516. Authorization for interception of wire or oral communications.
2517. Authorization for disclosure and use of intercepted wire or oral communications.
2518. Procedure for interception of wire or oral communications.
2519. Reports concerning intercepted wire or oral communications.
2520. Recovery of civil damages authorized.

AMENDMENTS

1970—Pub. L. 91-452, title II, § 227(b), Oct. 15, 1970, 84 Stat. 930, struck out item 2514 "Immunity of witnesses", which section was repealed four years following the sixtieth day after Oct. 15, 1970.

1968—Pub. L. 90-351, title III, § 802, June 19, 1968, 82 Stat. 212, added chapter 119 and items 2510-2520.

CHAPTER REFERRED TO IN OTHER SECTIONS

This chapter is referred to in title 47 section 605.

CHAPTER REFERRED TO IN D.C. CODE

This chapter is referred to in section 23-556 of the District of Columbia Code.

§ 2510. Definitions.

As used in this chapter—

(1) "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device.

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire or oral communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means—

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire or oral communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code; and

(11) "aggrieved person" means a person who was a party to any intercepted wire or oral communication or a person against whom the interception was directed.

(Added Pub. L. 90–351, title III, § 802, June 19, 1968, 82 Stat. 212.)

CONGRESSIONAL FINDINGS

Section 801 of Pub. L. 90–351 provided that:

"On the basis of its own investigations and of published studies, the Congress makes the following findings:

"(a) Wire communications are normally conducted through the use of facilities which form part of an interstate network. The same facilities are used for interstate and intrastate communications. There has been extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversation. Electronic, mechanical, and other intercepting devices are being used to overhear oral conversations made in private, without the consent of any of the parties to such communications. The contents of these communications and evidence derived therefrom are being used by public and private parties as evidence in court and administrative proceedings, and by persons whose activities affect interstate commerce. The possession, manufacture, distribution, advertising, and use of these devices are facilitated by interstate commerce.

"(b) In order to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceedings, and to prevent the obstruction of interstate commerce, it is necessary for Congress to define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized, to prohibit any unauthorized interception of such communications, and the use of the contents thereof in evidence in courts and administrative proceedings.

"(c) Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice.

"(d) To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused."

NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE

Section 804 of Pub. L. 90–351, as amended by Pub. L. 91–644, title VI, § 20, Jan. 2, 1971, 84 Stat. 1892, provided that:

"(a) [ESTABLISHMENT] There is hereby established a National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance (hereinafter in this section referred to as the 'Commission').

"(b) [MEMBERSHIP] The Commission shall be composed of fifteen members appointed as follows:

"(A) Four appointed by the President of the Senate from Members of the Senate;

"(B) Four appointed by the Speaker of the House of Representatives from Members of the House of Representatives; and

"(C) Seven appointed by the President of the United States from all segments of life in the United States including lawyers, teachers, artists, businessmen, newspapermen, jurists, policemen, and community leaders, none of whom shall be officers of the executive branch of the Government.

"(c) [CHAIRMAN; VACANCIES] The President of the United States shall designate a Chairman from among the members of the Commission. Any vacancy in the Commission shall not affect its powers but shall be filled in the same manner in which the original appointment was made.

"(d) [FUNCTION] It shall be the duty of the Commission to conduct a comprehensive study and review of the operation of the provisions of this title, in effect on the effective date of this section, to determine the effectiveness of such provisions during the six-year period immediately following the date of their enactment.

"(e) [PERSONNEL; APPOINTMENT, COMPENSATION AND QUALIFICATIONS] (1) Subject to such rules and regulations as may be adopted by the Commission, the Chairman shall have the power to—

"(A) appoint and fix the compensation of an Executive Director, and such additional staff personnel as he deems necessary, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, but at rates not in excess of the maximum rate for GS–18 of the General Schedule under section 5332 of such title; and

"(B) procure temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code, but at rates not to exceed $100 a day for individuals.

"(2) In making appointments pursuant to paragraph (1) of this subsection, the Chairman shall include among his appointment individuals determined by the Chairman to be competent social scientists, lawyers, and law enforcement officers.

"(f) [COMPENSATION, TRAVEL AND OTHER EXPENSES] (1) A member of the Commission who is a Member of Congress shall serve without additional compensation, but shall be reimbursed for travel, subsistence, and other necessary expenses incurred in the performance of duties vested in the Commission.

"(2) A member of the Commission from private life shall receive $100 per diem when engaged in the actual performance of duties vested in the Commission, plus reimbursement for travel, subsistence, and other necessary expenses incurred in the performance of such duties.

"(g)(1) The Commission or any duly authorized subcommittee or member thereof may, for the purpose of carrying out the provisions of this title, hold such hearings, sit and act at such times and places, administer such oaths, and require by subpena or otherwise the attendance testimony of such witnesses and the production of such books, records, correspondence, memorandums, papers and documents as the Commission or such subcommittee or member may deem advisable. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission or before such subcommittee or member. Subpenas may be issued under the signature of the Chairman or any duly designated member of the Commission, and may be served by any person designated by the Chairman or such member.

"(2) In the case of contumacy or refusal to obey a subpena issued under subsection (1) by any person who

resides, is found, or transacts business within the jurisdiction of any district court of the United States, the district court, at the request of the Chairman of the Commission, shall have jurisdiction to issue to such person an order requiring such person to appear before the Commission or a subcommittee or member thereof, there to produce evidence if so ordered, or there to give testimony touching the matter under inquiry. Any failure of any such person to obey any such order of the court may be punished by the court as a contempt thereof.

"(3) The Commission shall be 'an agency of the United States' under subsection (1), section 6001, title 18, United States Code for the purpose of granting immunity to witnesses.

"(4) Each department, agency, and instrumentality of the executive branch of the Government, including independent agencies, is authorized and directed to furnish to the Commission, upon request made by the Chairman, on a reimbursable basis or otherwise, such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this title. The Chairman is further authorized to call upon the departments, agencies, and other offices of the several States, to furnish, on a reimbursable basis or otherwise, such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this title.

"(h) [REPORTS TO PRESIDENT AND CONGRESS; TERMINATION DATE] The Commission shall make such interim reports as it deems advisable, and it shall make a final report of its findings and recommendations to the President of the United States and to the Congress within the two-year period following the effective date of this subsection. Sixty days after submission of its final report, the Commission shall cease to exist.

"(i) [CONFLICT OF INTEREST; EXEMPTION] (1) Except as provided in paragraph (2) of this subsection, any member of the Commission is exempted, with respect to his appointment, from the operation of sections 203, 205, 207, and 209 of title 18, United States Code.

"(2) The exemption granted by paragraph (1) of this subsection shall not extend—

"(A) to the receipt of payment of salary in connection with the appointee's Government service from any source other than the private employer of the appointee at the time of his appointment, or

"(B) during the period of such appointment, to the prosecution, by any person so appointed, of any claim against the Government involving any matter with which such person, during such period, is or was directly connected by reason of such appointment.

"(j) [APPROPRIATIONS] There is authorized to be appropriated such sum as may be necessary to carry out the provisions of this section.

"(k) [EFFECTIVE DATE] The foregoing provisions of this section shall take effect upon the expiration of the fifth year period immediately following the date of the enactment of this Act [June 19, 1968]."

REPEAL

Sec. 1212 of the Act of Oct. 15, 1970, Pub. L. 91–452, repealed sec. 804 of the Act of July 19, 1968, Pub. L. 90–351.

However, section 20 of the Act of Jan. 2, 1971, Pub. L. 91–644, repealed Sec. 1212 of Pub. L. 91–452 and contained certain amendments to section 804 of Pub. L. 90–351, which are set out above.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in section 3504 of this title

§ 2511. Interception and disclosure of wire or oral communications prohibited.

(1) Except as otherwise specifically provided in this chapter any person who—

(a) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire or oral communication;

(b) willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) willfully discloses, or endeavors to disclose, to any other person the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection; or

(d) willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection;

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2) (a) (i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: *Provided*, That said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) It shall not be unlawful under this chapter for an officer, employee, or agent of any communication common carrier to provide information, facilities, or technical assistance to an investigative or law enforcement officer who, pursuant to this chapter, is authorized to intercept a wire or oral communication.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United

States Code, to intercept a wire communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act.

(3) Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power. (Added Pub. L. 90–351, title III, § 802, June 19, 1968, 82 Stat. 213, and amended Pub. L. 91–358, title II, § 211(a), July 29, 1970, 84 Stat. 654.)

AMENDMENTS

1970—Subsec. (2)(a). Pub. L. 91–358 designated existing provisions as cl. (i), and added cl. (ii).

EFFECTIVE DATE OF 1970 AMENDMENT

Section 901(a) of Pub. L. 91–358 provided in part that the amendment of this section by Pub. L. 91–358 shall take effect on the first day of the seventh calendar month which begins after July 29, 1970.

§ 2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited.

(1) Except as otherwise specifically provided in this chapter, any person who willfully—

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication any advertisement of—

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire or oral communications,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) a communications common carrier or an officer, agent, or employee of, or a person under contract with, a communications common carrier, in the normal course of the communications common carrier's business, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications.

(Added Pub. L. 90–351, title III, § 802, June 19, 1968, 82 Stat. 214.)

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in section 2513 of this title.

§ 2513. Confiscation of wire or oral communication intercepting devices.

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of

compensation to informers in respect of such forfeitures, shall appy to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General. (Added Pub. L. 90–351, title III, § 802, June 19, 1968, 82 Stat. 215.)

§ 2514. Immunity of witnesses.

Whenever in the judgment of a United States attorney the testimony of any witness, or the production of books, papers, or other evidence by any witness, in any case or proceeding before any grand jury or court of the United States involving any violation of this chapter or any of the offenses enumerated in section 2516, or any conspiracy to violate this chapter or any of the offenses enumerated in section 2516 is necessary to the public interest, such United States attorney, upon the approval of the Attorney General, shall make application to the court that the witness shall be instructed to testify or produce evidence subject to the provisions of this section, and upon order of the court such witness shall not be excused from testifying or from producing books, papers, or other evidence on the ground that the testimony or evidence required of him may tend to incriminate him or subject him to a penalty or forfeiture. No such witness shall be prosecuted or subjected to any penalty or forfeiture for or on account of any transaction, matter or thing concerning which he is compelled, after having claimed his privilege against self-incrimination, to testify or produce evidence, nor shall testimony so compelled be used as evidence in any criminal proceeding (except in a proceeding described in the next sentence) against him in any court. No witness shall be exempt under this section from prosecution for perjury or contempt committed while giving testimony or producing evidence under compulsion as provided in this section. (Added Pub. L. 90–351, title III, § 802, June 19, 1968, 82 Stat. 216.)

REPEAL

Pub. L. 91–452, title II, §§ 227(a), 260, Oct. 15, 1970, 84 Stat. 930, 931, repealed this section effective four years following the sixtieth day after the date of the enactment of Pub. L. 91–452, which was approved Oct. 15, 1970, with such repeal not to affect any immunity to which any individual is entitled hereunder by reason before such day. See section 260 of Pub. L. 91–452, set out as a note under section 6001 of this title.

CROSS REFERENCES

Immunity of witnesses, see section 6001 et seq. of this title.

§ 2515. Prohibition of use as evidence of intercepted wire or oral communications.

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter. (Added Pub. L. 90–351, title III, § 802, June 19, 1968, 82 Stat. 216.)

§ 2516. Authorization for interception of wire or oral communications.

(1) The Attorney General, or any Assistant Attorney General specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), or chapter 102 (relating to riots);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1084 (transmission of wagering information), section 1503 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential assassinations, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), sections 2314 and 2315 (interstate transportation of stolen property), section 1963 (violations with respect to racketeer influenced and corrupt organizations)

or section 351 (violations with respect to congressional assassination, kidnaping, and assault);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving bankruptcy fraud or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title; or

(g) any conspiracy to commit any of the foregoing offenses.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire or oral communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire or oral communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses. (Added Pub. L. 90–351, title III, § 802, June 19, 1968, 82 Stat. 216, and amended Pub. L. 91–452, title VIII, § 810, title IX, § 902(a), title XI, § 1103, Oct. 15, 1970, 84 Stat. 940, 947, 959; Pub. L. 91–644, title IV, § 16, Jan. 2, 1971, 84 Stat. 1891.)

AMENDMENTS

1971—Par. (1)(c). Pub. L. 91–644 added provision authorizing interception of communications with respect to section 351 offense (violations with respect to congressional assassination, kidnaping, and assault).

1970—Par. (1)(c). Pub. L. 91–452 added provisions authorizing applicability to sections 844(d), (e), (f), (g), (h), or (i), 1511, 1955, and 1963 of this title.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 2514, 2518 of this title.

§ 2517. Authorization for disclosure and use of intercepted wire or oral communications.

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire or oral communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire or oral communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable. (Added Pub. L. 90–351, title III, § 802, June 19, 1968, 82 Stat. 217, and amended Pub. L. 91–452, title IX, § 902(b), Oct. 15, 1970, 84 Stat. 947.)

AMENDMENTS

1970—Par. (3). Pub. L. 91–452 substituted "proceeding held under the authority of the United States or of any State or political subdivision thereof" for "criminal proceeding in any court of the United States or of any State or in any Federal or State grand jury proceeding".

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in section 2518 of this title.

§ 2518. Procedure for interception of wire or oral communications.

(1) Each application for an order authorizing or approving the interception of a wire or oral communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication

is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire or oral communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire or oral communications within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) there is probable cause for belief that the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire or oral communication shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire or oral communication shall, upon request of the applicant, direct that a communication common carrier, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such carrier, landlord, custodian, or person is according the person whose communications are to be intercepted. Any communication common carrier, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant at the prevailing rates.

(5) No order entered under this section may authorize or approve the interception of any wire or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(a) an emergency situation exists with respect to conspiratorial activities threatening the na-

tional security interest or to conspiratorial activities characteristic of organized crime that requires a wire or oral communication to be intercepted before an order authorizing such interception can with due diligence be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire or oral communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8) (a) The contents of any wire or oral communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire or oral communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire or oral communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire or oral communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any intercepted wire or oral communication or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10) (a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that—

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes

of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted. (Added Pub. L. 90–351, title III, § 802, June 19, 1968, 82 Stat. 218, and amended Pub. L. 91–358, title II, § 211(b), July 29, 1970, 84 Stat. 654.)

AMENDMENTS

1970—Subsec. (4). Pub. L. 91–358 added the provision that, upon the request of the applicant, an order authorizing the interception of a wire or oral communication direct that a communication common carrier, landlord, custodian, or other person furnish the applicant with all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services provided.

EFFECTIVE DATE OF 1970 AMENDMENT

Section 901(a) of Pub. L. 91–358 provided in part that the amendment of this section by Pub. L. 91–358 shall take effect on the first day of the seventh calendar month which begins after July 29, 1970.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 2516, 2519, 2520 of this title.

§ 2519. Reports concerning intercepted wire or oral communications.

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for;

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire or oral communications and the number of orders and extensions granted or denied during the preceding calendar year. Such reports shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section. (Added Pub. L. 90–351, title III, § 802, June 19, 1968, 82 Stat. 222.)

SECTION REFERRED TO IN D.C. CODE

This section is referred to in section 23–555 of the District of Columbia Code.

§ 2520. Recovery of civil damages authorized.

Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person—

(a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

(b) punitive damages; and

(c) a reasonable attorney's fee and other litigation costs reasonably incurred.

A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law. (Added Pub. L. 90–351, title III, § 802, June 19, 1968, 82 Stat. 223, and amended Pub. L. 91–358, title II, § 211(c), July 29, 1970, 84 Stat. 654.)

AMENDMENTS

1970—Pub. L. 91–358 substituted provisions that a good faith reliance on a court order or legislative authorization constitute a complete defense to any civil or criminal action brought under this chapter or under any other law, for provisions that a good faith reliance on a court

order or on the provisions of section 2518(7) of this chapter constitute a complete defense to any civil or criminal action brought under this chapter.

EFFECTIVE DATE OF 1970 AMENDMENT

Section 901(a) of Pub. L. 91-358 provided in part that the amendment of this section by Pub. L. 91-358 shall take effect on the first day of the seventh calendar month which begins after July 29, 1970.

CRS
CRS
CRS
CRS
CRS
CRS
CRS
CRS
CRS
CRS
CRS
CRS
CRS

CONGRESSIONAL RESEARCH SERVICE
LIBRARY OF CONGRESS

CRS

BIBLIOGRAPHY

ON

COMPUTERS, PRIVACY,
GOVERNMENT INFORMATION
AND RELATED MATTERS

SELECTED FROM THE

CRS BIBLIOGRAPHIC DATA BASE

CREATED AND MAINTAINED
BY
LIBRARY SERVICES DIVISION

DATES COVERED: 1/1/69-7/15/76
NO. OF CITATIONS: 311
TYPE OF CATALOG: Author
CATALOG NUMBER: 6-7-21

Albergotti, Robert D.
Search and seizure--warrantless foreign national security, wiretaps. Tulane law review, v. 49, May 1975: 1153-1160.
Case note reviews Federal appellate decision holding "that warrantless electronic surveillance authorized by the executive branch for the purpose of gathering foreign intelligence information was not illegal; thus, disclosure to defendant was not required."

Alexander, Theron.
Social controls and the individual; a psychological analysis of the invasion of privacy. Intellect, v. 103, Oct. 1974: 41-44.
"There must be an establishment of a basic trust between the individual and the organizations of society."

Amsterdam, Anthony G.
Perspectives on the Fourth Amendment. Minnesota law review, v. 58, Jan. 1974: whole issue.
Article considers "(a) the scope of application of the fourth amendment, that is, the kinds of law enforcement activities to which it applies; (b) the restrictions that the fourth amendment imposes upon those activities; and (c) the use of the exclusionary rule to enforce the restrictions."

Andrews, Frederick T., Jr. Boyd, Richard C.
The Bell System and global communications. Bell Laboratories record, v. 52, Jan. 1974: 3-11.
"Bell System engineers are working with couterparts from many countries throughout the world to help make telephone systems mutually compatible. Their major achievements include agreements in direct overseas dialing for voice transmission and on international data communications."

Arbib, Michael A.
Man-machine symbiosis and the evolution of human freedom. American scholar, v. 43, winter 1973-1974: 38-54.
Suggests ways technology in general, and computers in particular can be used to solve society's problems.

Arner, Paul.
Computer technology and surveillance. Computers and people, v. 24, Sept. 1975: 8-11.
Points out the rapid advances in electronics technology that would make it easy to develop computer systems for maintaining surveillance on private citizens.

Aronoff, Stanley.
The politics of privacy. Ripon forum, v. 10, Jan. 1974: 5-7.
"Ohio State Sen. Stanley Aronoff (R) served on the Department of Health, Education, and Welfare Advisory Committee on Automated Personal Data Systems which issued its report on computer data banks in 1973. In this article, the Cincinnati legislator suggests that state and federal legislation should be enacted to limit computer intrusion into personal privacy."

Aronoff, Stanley J.
1984--only 11 years away. State government, v. 46, spring 1973: 66-75.
Asserts that expanding private and public record keeping, assisted by computerization, constitutes a threat to the right of privacy. Because revenue sharing may make state and local governments the Nation's "primary information hounds," the author recommends that the states "take affirmative action to come to grips with the problems of records and data banks."

Association of the Bar of the City of New York. Committee on Civil Rights.
The Central Intelligence Agency: oversight and accountability. [New York] Association of the Bar of the City of New York, 1975. 46 p.
This report "(1) summarizes the creation and legal development of the CIA, (2) discusses the CIA's domestic activities and their relation to the laws governing the Agency and to the Constitution, (3) discusses the foreign activities of the CIA and the legislative and constitutional basis for these activities, (4) describes the present funding arrangements of the Agency and their legal basis, and (5) discusses possible remedies and makes recommendations concerning regulation of the CIA's activities in the future."

Association of the Bar of the City of New York. Committee on Civil Rights.
Military surveillance of civilian political activities: report and recommendations for congressional action. Record of the Association of the Bar of the City of New York, v. 28, Oct. 1973: 651-676.
Committee report examines the background and current status of and legal considerations involved in domestic intelligence operations by the military and concludes "that Congress should enact legislation to prohibit all military surveillance of civilian political activities, except perhaps in certain well-defined circumstances where limited data-gathering may be justifiable."

Association of the Bar of the City of New York. Committee on Civil Rights.
The privacy of Federal income tax returns; committee report. Record of the Association of the Bar of the City of New York, v. 30, May-June 1975: 400-408.
Analyzes the statutes, judicial decisions, Executive Orders, and proposed new legislation (S. 199) relevant to the tax return privacy issue. Passage of S. 199 with amendment is recommended.

Association of the Bar of the City of New York. Committee on Federal Legislation.
Government databanks and privacy of individuals (H.R. 16373 and S. 3418). Record of the Association of the Bar of the City of New York, v. 30, Jan.-Feb. 1975: 55-106.
"This report has two objectives. The first is to identify general principles which can and should be adopted to regulate databanks for the purposes of protecting individual privacy and of assuring fairness to the individual in the decision-making process insofar as it is based on information about him contained in databanks. The second is to offer our comments and suggestions regarding the current House and Senate bills."

Association of the Bar of the City of New York. Committee on Federal Legislation.
Judicial procedures for national security electronic surveillance. Record of the Association of the Bar of the City of New York, v. 29, Dec. 1974: 751-774.
Recommends, with modification, passage of the Surveillance Practices and Procedures Act, which would "establish judicially-administered procedures with which the Government must comply when initiating and maintaining electronic surveillance in national security matters."

Association of the Bar of the City of New York. Committee on Labor and Social Security Legislation.
The polygraph in employment: the consequences of its search for truth. Record of the Association of the Bar of the City of New York, v. 28, June 1973: 464-480.
Recommends prohibition of the use of the polygraph in public and private employment situations.

Autonomy plus electronics: an effective combination. Government executive, v. 7, June 1975: 15, 18, 22, 26.
"The Onondaga Law Enforcement Mobile Radio District advantages easily outweigh those of any individual agency communications systems: system delivers massive computer information power into the hands of the operating patrolman."

Ball, John H.
The development to a code of police ethical practice: some perspectives and problems. Police chief, v. 41, Jan. 1974: 20, 23.
Describes the work being done by the Law Enforcement Association on Professional Standards, Education and Ethical Practice (LEAPS).

Bancroft, T. A.
The statistical community and the protection of privacy. American statistician, v. 26, Oct. 1972: 13-16.
Considers the protection of privacy in its relation to the statistical community with regard to the data programs of the Federal Government.

Bank Secrecy Act violates the Fourth Amendment. Texas law review, v. 51, Mar. 1973: 602-612.
Case note reviews a Federal District Court opinion which held that the requirement of the Bank Secrecy Act for financial institutions to report all domestic transactions over $10,000 violates the customer's right of privacy.

Banner, Conrad S. Stock, Robert H.
The FBI's approach to automatic fingerprint identification. FBI law enforcement bulletin, v. 44, Jan. 1975: 2-9.
Outlines the development of the FBI's research project.

Barks, Dennis.
Right of privacy--availability of injunctive relief for invasions of privacy. Missouri law review, v. 39, fall 1974: 647-658.
Comment surveys common patterns of conduct which have been held to be impermissible invasions of the right of privacy, concluding that such invasions should be subject to injunction.

Baron, William A.
Voiceprint identification: the trend towards admissibility. New England law review, v. 9, spring 1974: 419-432.
Comment finds that the "trend since 1971 has most decidedly been to admit voiceprint evidence, at least for the purpose of corroboration, yet few courts of last resort have ruled on this question."

Baskir, Lawrence M.
Reflections on the Senate investigation of Army surveillance. Indiana law journal, v. 49, summer 1974: 618-653.
This article describes how the Subcommittee on Constitutional Rights of the Senate Judiciary Committee conducted its investigation of a bill proposed by Sen. Ervin "to amend existing prohibitions on military involvement in civilian political affairs by creating a criminal prohibition against the collection of information on political activities of American civilians not affiliated with the military."

Becker, Louise Giovane.
Congressional interest in security and privacy of criminal justice information systems. In Carnahan Conference on Crime Countermeasures, Lexington, Ky., 1975. Proceedings. [Lexington, College of Engineering, University of Kentucky] 1975. p. 1-8.
Examines some of the legislative remedies and proposals to establish policies and safeguards to protect information in computerized criminal justice systems from misuse.

Becker, R. W., and others.
A semiautomatic speaker recognition system. [Washington] U.S. Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, 1973. 68 p.
"Speaker recognition is the act of naming, identifying, or distinguishing from other speakers the speaker who has produced a given voice sample." "The performance of this computer-based system is sufficiently good to justify the use of such systems by law enforcement agencies. The prototype system is faster and requires much lower operator skill levels than methods using visual comparisons of spectrograms."

Berkon, Frederick D. Yates, John J.
An allegation of a chilling effect on First Amendment freedoms is not sufficient to create a justiciable controversy in the absence of a concrete showing of present objective harm or threat of specific future harm. George Washington law review, v. 41, Dec. 1972: 385-395.
Case note discusses Laird v. Tatum which set forth a standard justiciability.

Blanc, R. P., and others.
Annotated bibliography of the literature on resource sharing computer networks. [Washington] U.S. National Bureau of Standards [for sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1973. 90 p. (U.S. National Bureau of Standards. Special publication 384)

Bleiberg, Robert M.
"Economic nudity"; the Bank Secrecy Act is a chilling threat to freedom. Barron's, June 26, 1972: 7.
"In guise of fighting white-collar crime, would subject law-abiding to massive invasion of privacy. Pete Stark and the ACLU may hold strange views about a lot of things, but here they have shown the Establishment the way."

Bloustein, Edward J.
The First Amendment and privacy: the Supreme Court justice and the philosopher. Rutgers law review, v. 28, fall 1974: 41-95.
Article examines the philosophical basis for reconciling freedom of the press with the right to legal protection against invasion of privacy by mass publication.

Bouvard, Marguerite Guzman. Bouvard, Jacques.
Computerized information and effective protection of individual rights. Society, v. 12, Sept.-Oct. 1975: 62-67.
"Three significant privacy areas are still not covered by legislation: criminal justice records, data banks maintained by the private sector and state and local government responsibility for taxes and welfare records."

Braunstein, Michael.
Constitutional law--jurisdiction of Federal courts--First Amendment chill resulting from Army surveillance non-justiciable. Tulane law review, v. 47, Feb. 1973: 426-436.
Case note on Laird v. Tatum in which the Supreme Court held "that a claim predicated on the chilling of first amendment rights by executive action short of a direct restraint, and arising merely from the individual's perception of that action, was non-justiciable."

Bricker, Paul.
The voiceprint technique: a problem in scientific evidence. Wayne law review, v. 18, July-Aug. 1972: 1365-1402.
Comment considers the voiceprint method of speaker identification, using aural and visual examination, which is the only technique "presently available with a scientific basis establishing a sufficiently high degree of accuracy to permit expert identification...in judicial proceedings;" focuses on reliability and "current scientific and legal opinion."

Brown, Peter Northrop.
Guilt by physiology: the constitutionality of tests to determine predisposition to violent behavior. Southern California law review, v. 48, Nov. 1974: 489-570.
Surveys current biotechnical research to develop a testing program to identify persons bearing organic correlates of violent behavior, examines the Center for the Study and Reduction of Violence at the University of California, Los Angeles, which is pursuing such a program, and discusses the constitutionality of a mass screening program to identify people predisposed to violent behavior.

Bruining, Henry.
Law Enforcement Code of Ethics. Police chief, v. 40, Oct. 1973: 68, 238, 240.
Analyzes the Law Enforcement Code of Ethics.

Bulger, John P.
Tactical sensors for the Army. National defense, v. 60, Jan.-Feb. 1976: 279-281.
"Due to developments that were brought about by the conflict in Vietnam the American soldier is now able to detect the approach of enemy troops and vehicles with accuracy over long distances."

Butterfield, Mary Bolner. Colman, Ronald.
The right of privacy in an open society (bibliography series number thirty-three). Readers advisory service, v. 2, 1975: 94-1 - 94-9.
Annotated selected listing including works on surveillance techniques and record keeping, business, the media, voluntary associations, police agencies, and governmental agencies.

Callahan, W. Thomas. Knoblauch, Richard L.
Criminal justice research: prevention and control of collective violence. [Washington] National Institute of Law Enforcement and Criminal Justice [for sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1973. 1 v. (various pagings)
Vol. 3--Guidelines for intelligence personnel.

Campaigne, Howard. Hoffman, Lance J.
Computer privacy and security. Computers and automation, v. 22, July 1973: 12-17.
"Several firms are now marketing as standard products bulk memories which could store a one-page dossier on each of the 200 million citizens of the United States in...about 225 square feet. In one system...all of these dossiers could be available on-line, with an access time of approximately 6 seconds."

Carey, Sarah C.
Students, parents and the school record prison: a legal strategy for preventing abuse. Journal of law & education, v. 3, July 1974: 365-388.
Article outlines a number of legal theories to insure parental access to student records and to deny outside agency access.

Carnahan and International Crime Countermeasures Conference, April 16-19, 1974, proceedings. [Lexington, ORES Publications, College of Engineering, University of Kentucky, 1974] 268 p.
"74 CHO 868-0 AES"
Partial contents.--Current status of fence intrusion detection systems, by T. Kabaservice, and others.--Standards for law enforcement equipment, by R. Mills.--The effect of technology on the police officer, by E. Zannes.--A computerized communications system for emergency services, by J. Barnes and R. Carter.--The courtroom of the future, by J. Richmond.--A civilian system for emergency communication and mobility, by J. Jackson.--Computers and crime, by R. Abbott.

Carnahan Conference on Crime Countermeasures, Lexington, Ky., 1975.
Proceedings. [Lexington, College of Engineering, University of Kentucky] 1975. 200 p.
Partial contents.--An evaluation of the benefits of automated command and control system, by S. Riter and others.--Law enforcement armed robbery alarm system utilizing recorded voice addresses via police radio channels, by S. Daskam.--Automatic speaker recognition by computers, by E. Bunge.--Politics and police communications systems, by E. Zannes.--The application of crime countermeasures for the protection of nuclear materials, by C. Bean.--The position of the independent testing laboratory in the evaluation of security equipment and systems, by R. McCleary.

Carnahan Conference on Electronic Crime Countermeasures, Lexington, Ky., 1973.
Proceedings. [Lexington, College of Engineering, University of Kentucky] 1973. 176 p.
"UKY BU102"

Carpinello, Anthony J.
Electronic surveillance by bugged agents is not a search and seizure within the Fourth Amendment--United States v. White. Albany law review, v. 36, no. 2, 1972: 451-458.
A discussion of the historical limits of search and seizure and when a search warrant is not needed.

Cassin, Rene.
Science and human rights. Impact of science on society, v. 22, Oct.-Dec. 1972: 329-339.
"The camera, the computer, surgical adventure, the microphone, toxic or tranquillizing chemicals can be made to trespass on the human right to a decent life. Man needs to take a legal and moral stand on such important issues of conscience while still deriving the best from science."

Cherry, William A.
The military: a source of equipment and training. Police chief, v. 42, Apr. 1975: 53-55.
Details aid in "the form of training, loans of equipment, and personnel to civilian police departments" by the military.

Christie, George C.
Government surveillance and individual freedom: a proposed statutory response to Laird v. Tatum and the broader problem of government surveillance of the individual. New York University law review, v. 47, Nov. 1972: 871-902.
Article proposes a statute regulating military and civilian law enforcement agency surveillance. The author "makes an effort to balance the seemingly conflicting objectives of those who emphasize society's need for security and those who emphasize the individual's need for privacy."

The CIA's secret funding and the Constitution. Yale law journal, v. 84, Jan. 1975: 608-636.

Cohn, Sigmund A.
"Criminal records"--a comparative approach. Georgia journal of international & comparative law, v. 4, winter 1974: 116-156.
Compares the American practice of disseminating arrest records with procedures in Switzerland, France, Italy, and West Germany.

Colby, Jonathan E.
The developing international law on gathering and sharing security intelligence. Yale studies in world public order, v. 1, no. 1, 1974: 49-92.
"Although nation-states have not repealed their statutes or otherwise abandoned their policies against the performance of security intelligence function within their national territory by operatives of another state, there is evidence of increasing recognition on their part of the significance to their collective security of greater sharing of security intelligence and of opportunities to gather such information. Support for such a trend is found in the practice of nations exchanging their intelligence gathering operatives held by one another, levying less than maximal sentences on captured operatives of another, and acknowledging their sponsorship of intelligence gathering activities within the territory of other states."

Colton, Kent W.
Computers and the police: police departments and the new information technology. Urban data service, v. 6, Nov. 1974: 1-19.
Measures the extent of police computer use for law enforcement purposes and the extent of success or failure of such systems.

Constitutional law--a right of privacy in photographs and fingerprints. New York law forum, v. 17, no. 4, 1972: 1126-1132.
Comment considers Eddy v. Moore, in which there was "recognition of a constitutional right of privacy in fingerprints and photographs taken at the time of arrest once the charge on which the arrest was based has been dismissed."

Cook, Daniel F.
Electronic surveillance, title III, and the requirement of necessity. Hastings constitutional law quarterly, v. 2, spring 1975: 571-618.
"Title III of the Omnibus Crime Control and Safe Streets Act of 1968 requires a showing that electronic surveillance is 'necessary' before it can be judicially authorized. The [student] author examines the constitutional basis for the necessity requirement and analyzes the judicial decisions which have construed it. Finding no case holding the requirement has not been met, he concludes that it has been severely undercut."

Cook, Joseph G.
Requisite particularity in search warrant authorizations. Tennessee law review, v. 38, summer 1971: 496-516.
"The present article is concerned with several aspects of this requirement of particularity. First, attention will be directed to problems regarding the description of the place to be searched. Second, consideration will be given to the itemization of the objects to be seized, and the possibility of seizing additional items has enumerated. Finally, the unique problems presented by the application of this language of the fourth amendment to electronic eavesdropping will be explored."

Coolidge, Hermann W., Jr.
Electronic surveillance--the problem of subsequent justification. Mercer law review, v. 23, summer 1972: 989-993.
Case note.

Costner, Thomas E. Grimmer, John E.
Search and seizure of bank records and reports. Banking law journal, v. 92, Apr. 1975: 347-358.
"This article examines the search and seizure ramifications of the Bank Secrecy Act as elucidated by the recent Supreme Court opinion, California Bankers Association v. Shultz, and related lower court opinions."

Countryman, Vern.
Computers and dossiers--part II. Computers and automation, v. 21, Feb. 1972: 14-20, 36.

Countryman, Vern.
The diminishing right of privacy: the personal dossier and the computer. Texas law review, v. 49, May 1971: 837-882.
The author "urges that preservation of privacy demands sweeping congressional reevaluation of society's need for such files and suggests that those not serving 'an actual need for a vital public purpose' be done away with."

The Court and electronic surveillance: to bug or not to bug--what is the exception? St. John's law review, v. 47, Oct. 1972: 76-106.
Comment overviews the development by the Supreme Court of Fourth Amendment restraints on the power of government to engage in electronic surveillance.

Courtney, Jeremiah.
Electronic eavesdropping, wiretapping and your right of privacy. Federal communications bar journal, v. 26, 1973: 1-60.
Article attempts "to evaluate the collision course that wiretapping and electronic eavesdropping appear to be running against the individual's right of privacy."

Coyle, Robert E.
Surveillance from the seas. Military law review, v. 60, spring 1973: 75-97.
"This comment will examine surveillance activities with a view toward defining what is or should be permissible under international law."

Curran, William J., and others.
Protection of privacy and confidentiality. Science, v. 182, Nov. 23, 1973: 797-802.
"Unique law protects patient records in a multistate psychiatric information system."

DeLong, Edward K.
The activities of the Central Intelligence Agency, at six billion dollars a year. Computers and automation, v. 21, Feb. 1972: 38-40.
"How a one-time professor, Victor Marchetti, spent fourteen years in the CIA, and resigned--after seeing much he did not like in the clandestine attitude, the amorality, and the distortion of intelligence for the benefit of special interests."

Dershowitz, Alan.
Unchecked wiretapping; before Watergate and after. New republic, v. 172, May 31, 1975: 13-17.
Charges that government wiretapping allegedly conducted for national security purposes "today is simply out of control, and it is entirely possible that we have seen only the tip of the iceberg."

DeWeese, J. Taylor.
Giving the computer a conscience. Harper's magazine, v. 247, Nov. 1973: 14, 16-17.
"How to protect fifty million people in the FBI's new crime file."

Dickey, C. Lewis.
Securing the computer. Journal of systems management, v. 23, Feb. 1972: 8-10.
"The author examines the need for security within an EDP organization and recommends some preventive measures to minimize the vulnerability of an EDP system."

District of Columbia. Police Dept.
Report on the operations of the Intelligence Division. [Washington] 1975. 1 v. (various pagings)
Provides "a complete report of this department's Intelligence Division activities over the past several years..."

Donner, Frank.
Electronic surveillance: the national security game. Civil liberties review, v. 2, no. 3, 1975: 15-47.
Interprets the history of electronic surveillance at the Federal level as one of using alleged threats to national security as a pretext for institutionalizing the expansion of clandestine eavesdropping.

Donner, Frank J.
Political intelligence: cameras, informers, and files. Civil liberties review, v. 1, summer 1974: 8-25.
Discusses three practices widely used in accumulating intelligence on dissident political groups: photography of demonstrations and rallies; infiltration of organizations by informers; and storage of the data thus generated in files and dossiers.

Ege, Stephen M.
Electronic funds transfer: a survey of problems and prospects in 1975. Maryland law review, v. 35, no. 1, 1975: 3-56.
Article examines electronic funds transfer and Federal control through "branching" and "payment powers" limitations, communications issues, UCC payments provisions, antitrust law, right of privacy and other matters.

Ehlke, Richard.
Political surveillance and police intelligence gathering--rights, wrongs, and remedies. Wisconsin law review, v. 1972, no. 1, 1972: 175-199.
Comment considers Anderson v. Sills, which challenges the constitutionality of "current police practices of collecting and maintaining intelligence information."

Electronic eavesdropping: a victim's primer. Notre Dame lawyer, v. 49, Oct. 1973: 162-184.

Comment purposes "to survey the major case law on the subject of electronic surveillance, and to review the current statutory prohibitions against illicit electronic eavesdropping--in short, to provide a primer for the victims of illegal wiretapping and bugging in the United States."

Electronic eavesdropping: Watergate comes full circle. Congressional quarterly weekly report, v. 31, Aug. 25, 1973: 2321-2324.

Examines the role of electronic surveillance techniques in the Watergate affair and reviews the legal and legislative history of the practice in the United States, including the policy of the Nixon administration. Includes statistics of FBI national security wiretaps for each year since 1945 and court-approved Federal and state wiretaps since 1969.

Electronic reconnaissance in Vietnam. International defense review, v. 5, Aug. 1972: 358-362.

Electronic surveillance of the grand jury witness: deterring Fourth Amendment violations intended to produce conviction of someone other than the victim. University of Pennsylvania law review, v. 120, Jan. 1972: 546-573.

"After discussing the principal cases, this Comment will consider separately title III [of the Omnibus Crime Control and Safe Streets Act] and the fourth amendment exclusionary rule as expounded by the Supreme Court to determine whether they supply a basis for the application of the exclusionary rule to witnesses in grand jury procedings."

Elliff, John T.

The politics of domestic intelligence surveillance and civil liberties under the Nixon administration. [Washington] c1974. 37 l.

"Prepared for delivery at the 1974 Annual Meeting of the American Political Science Association, Palmer House, Chicago, Illinois, August 29-September 2, 1974."

Reviews "uses of domestic intelligence operations by the Nixon administration as they have been disclosed in the Watergate and impeachment investigations," and examines factors which may be considered as part of a study of the F.B.I. in its domestic intelligence role.

Ellison, James M.
A report from the wiretap subculture. Washington monthly, v. 7, Dec. 1975: 27-33.
Draws on the author's experience as writer/editor of training publications for two interlocking companies in Florida, Audio Intelligence Devices and the National Intelligence Academy, to illustrate how "the use of wiretapping for domestic surveillance goes hand in hand with a more general disrespect for the law." Audio Intelligence Devices is described as a manufacturer of electronic surveillance equipment, whose use is taught to police by the National Intelligence Academy.

Ervin, Sam J., Jr.
Privacy and government investigations. University of Illinois law forum, v. 1971, 1971: 137-153.
"A quiet America will not be a free America. Rather, it will be a spiritually lifeless America. For that reason I believe that this claim of an inherent executive branch power of investigation and surveillance on the basis of people's beliefs and attitudes may be more of a threat to our internal security than any enemies beyond our borders."

The FBI has an affirmative duty to take reasonable precautions to ensure the accuracy of the information contained in its criminal files. Texas law review, v. 53, Aug. 1975: 1308-1321.

The Federal Paperwork Commissioner's challenge. Bureaucrat, v. 4, Oct. 1975: 283-299.
Partial contents.--Ending Federal forms pollution, by T. McIntyre.--The Commission on Federal Paperwork: a mechanism for reform, by F. Horton.--Managing government paperwork, by A. Ricks.--Centralized control of Federal statistical reporting, by J. Duncan.--The right of privacy versus technological advance, by E. Dwyer.

Feistel, Horst.
Cryptography and computer privacy. Scientific American, v. 228, May 1973: 15-23.
"Computer systems in general and personal 'data banks' in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer."

Foreign security surveillance and the Fourth Amendment. Harvard law review, v. 87, Mar. 1974: 976-1000.
Comment concludes that no exception to the warrant requirement to engage in electronic surveillance should be created in cases where foreign powers are involved.

Gallagher, Edward J., III. Hollis, Robert M.
Federal decisions on the constitutionality of electronic surveillance legislation. American criminal law review, v. 11, spring 1973: 639-694.
Comment explores the constitutionality of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 re: electronic surveillance, and provides a history of electronic surveillance, legislation and legal cases.

Galloway, Alec.
A decade of U.S. reconnaissance satellites. Interavia, v. 27, Apr. 1972: 376-389.
Describes the technical progress of the spaceborne reconnaissance system.

Gates, Andrew L., III.
Arrest records--protecting the innocent: misuse of arrest records. Tulane law review, v. 48, Apr. 1974: 629-648.
Discusses the problems confronting persons who have been arrested, had the charge dismissed but still have an arrest record.

Goldstein, Richard M. Brodie, Mark S.
Commercial credit bureaus: the right to privacy and state action. American University law review, v. 24, winter 1975: 421-489.
Comment analyzes "the constitutional basis of the right to informational privacy in the context of credit reporting and [proposes] alternative theories of state action under which commercial credit bureaus would be bound by constitutional guarantees."

Goldstein, Robert C.
The costs of privacy. Datamation, v. 21, Oct. 1975: 65-69.
Discusses the costs of complying with right of privacy regulations for computer systems.

Goldstein, Robert C. Nolan, Richard L.
Personal privacy versus the corporate computer. Harvard business review, v. 53, Mar.-Apr. 1975: 62-70.
"Now is the time for your company to plan for costly changes needed to comply with laws aimed at eliminating the privacy-invasion threat of personal data systems."

Government information and the rights of citizens. Michigan law review, v. 73, May-June 1975: whole issue.
Partial contents.--The classification system.--Executive privilege.--The Freedom of Information Act.--State open-records laws.--State and proposed Federal open-meeting laws.--State law of privacy.--The Federal constitutional law of privacy.--Federal statutory protection of privacy prior to the Privacy Act of 1974.--The Privacy Act of 1974.

Greenawalt, Kent.
Legal protections of privacy. Washington, Office of Telecommunications Policy [1975] 130 p.
Evaluates the existing legal protections for individual privacy, with particular emphasis on issues of concern to the Domestic Council Committee on the Right of Privacy and the Office of Telecommunications Policy.

Halperin, Morton H.
National security and civil liberties. Foreign policy, no. 21, winter 1975-76: 125-160.
Sets forth standards "which should be applied to national security wiretapping in a way which would permit the intelligence services to gather information, if indeed it is useful and valuable to the national security of the United States, while safeguarding the constitutional rights of American citizens."

Hanlon, Joseph.
Boardroom electronic warfare. New scientist, v. 67, July 10, 1975: 65-69.
"As bugs become more sophisticated, so do the electronic countermeasures, in an escalating warfare that has led some electronic poachers to see more profit in gamekeeping." Appends an account of bugging a member of the British Parliament to demonstrate the ease with which this might be done.

Hanlon, Joseph.
Does privacy threaten research? New scientist, v. 62, July 4, 1974: 30-31.
"People may refuse to cooperate with researchers because of fear that what they tell will be used to harm them, warns a study group in a report published today. Radically tighter rules are needed to protect both researcher and subject. Joseph Hanlon, who was a member of the study group and wrote the final report, looks at the proposals and the discussions which produced them."

Hanlon, Joseph.
Spotlight on privacy thieves. New scientist, v. 59, Aug. 16, 1973: 394-395.
"Strong new controls for computer data banks are urged in an official US report issued two weeks ago with the blessing of two Cabinet members. The restrictions are much tighter than anything suggested in Britain."

Hanlon, Joseph.
The telephone tells all. New scientist, v. 67, July 17, 1975: 148-151.
Outlines the variety of telephone tapping devices and reviews countermeasures.

Hayden, Trudy.
Watching big brother. New scientist, v. 68, Nov. 27, 1975: 526-527.
"The U.S. government has 25000 databanks with personal information about identifiable individuals. Beginning this autumn, Americans have the right to examine, correct and, in some instances, control the uses of data in these files. But in Britain, where the government still refuses even to publish a white paper on privacy, citizens have no such rights."

Helms, Dennis J.
A guide to the new Federal rules governing the confidentiality of alcohol and drug abuse patient records. Contemporary drug problems, v. 4, fall 1975: 259-283.
Reviews the Federal rules and points out that "the right to know enables an individual citizen to obtain more information about himself from government, while the Rules prevent government and others from obtaining more information about the individual than they are deemed to need to know."

Hemphill, Stuart R.
Protection of privacy of computerized records in the National Crime Information Center. University of Michigan journal of law reform, v. 7, spring 1974: 594-614.
Comment assesses the social costs and benefits of the National Crime Information Center, concluding that operational controls are needed to safeguard individual privacy.

Hodges, David P.
Electronic visual surveillance and the Fourth Amendment: the arrival of big brother? Hastings constituional law quarterly, v. 3, winter 1976: 261-299.
"The latest law enforcement tool for clandestine surveillance of individuals suspected of crime, involves the use of miniature television cameras to observe and videotape activity in areas heretofore inaccessible to visual intrusion. The author [in this comment] explores the constitutional implications of electronic visual surveillance by analogy to the standards currently applicable to electronic eavesdropping. He concludes that present law enforcement needs fail to justify the use of this new surveillance technique, and proposes a statutory prohibition on its use for any purpose."

Hougan, Jim.
A surfeit of spies. Harper's magazine, v. 249, Nov. 1974: 51-54, 56, 58, 63-64, 66-67.
Examines the operations of private intelligence agencies, focusing on "International Intelligence, Inc. (Intertel), a mysterious firm whose activities have impinged on the affairs of Howard Hughes, Robert Maheu, Robert Vesco, the Plumbers, ITT, Bebe Rebozo, and even the Mafia. Indeed it has a particular contemporary relevance in that its very existence seems to have cast a shadow of paranoia over Richard Nixon--and, at least indirectly, contributed to the former President's political reversal."

House Republican Research Committee. Republican Task Force on Privacy.
House Republican Research Committee: recommendations of privacy task force, August 21, 1974. In Remarks of Barry M. Goldwater. Congressional record [daily ed.] v. 120, Sept. 12, 1974: H9235-H9238.
Includes the text of the Republican Task Force on Privacy's report issued on Aug. 21, 1974.

Hyland, William F.
Report on the New Jersey Wiretapping and Electronic Surveillance Control Act. [Trenton?] 1974. 1 v. (various pagings)
Reports on the six-year test period for the New Jersey Wiretapping and Electronic Surveillance Control Act of 1968, describing the law's current operation and impact.

International Electronic Crime Countermeasures Conference, 1st, Edinburgh, 1973.
Proceedings. [Lexington] College of Engineering, University of Kentucky [1973] 247 p.
Partial contents.--Metal detectors for police use.--Detection of clandestine eavesdropping devices.--High-security methods of reporting information.--The computer in the service of the police.--Motor vehicle antihijack system.--Engineering considerations in computer center security.

International Symposium on Criminal Justice Information and Statistics Systems, 2d, San Francisco, 1974.
Proceedings. [Sacramento, Calif., SEARCH Group] 1974. 699 p.
This Project SEARCH Symposium presents a series of working papers on a variety of topics related to the application of advanced technology to criminal justice, such as police, judicial, corrections, and juvenile information systems, national programs in telecommunications, reporting/analysis systems, etc.

Jackson, Janko.
A methodology for ocean surveillance analysis. Naval War College review, v. 27, Sept.-Oct. 1974: 71-89.
"The requirements for effective ocean surveillance extending the more familiar concepts of reconnaissance and intelligence were delineated as part of a 1970 CNO study undertaken at the Naval Research Laboratory. Aimed at the needs of 1975-1985, this study outlines a methodology for evaluating ocean surveillance data collection and distribution both on a global scale and on levels ranging from strategic nuclear detection to the monitor of enemy air sorties."

Janov, Gwenellen P.
Electronic surveillances--the President of the United States has no authority to conduct wiretaps to protect against domestic threats to the national security without a judicial warrant. George Washington law review, v. 41, Oct. 1972: 119-134.
Case note discusses United States v. United States District Court for the Eastern District of Michigan.

Jones, Philip R. Wilkerson, William R.
Preparing special education administrators. Theory into practice, v. 14, Apr. 1975: 105-109.
Reviews the work of the General-Special Education Administration Consortium in promoting innovative preparation programs for general and special education administrators.

Jones, William R.
Danger--voiceprints ahead. American criminal law review, v. 11, spring 1973: 549-573.
Article reviews "recent developments in both the scientific and legal communities in an attempt to give guidance on the question, 'should 'voiceprint' identification evidence be admitted at trial?'"

Judicial review of military surveillance of civilians: big brother wears modern Army green. Columbia law review, v. 72, Oct. 1972: 1009-1047.
"This Note focuses on the problems inherent in attempts to assert judicial control over the intelligence gathering activities of the military as exemplified by two recent cases."

Kelley, Clarence M.
But so is the right to law and order. Trial, v. 11, Jan.-Feb. 1975: 23, 27, 32.
FBI director discusses the file structure of the FBI and means by which information about citizens is gathered and stored, relating FBI procedure to the right of individual privacy.

Kelly, Thomas C. Ward, John E.
Investigation of digital mobile radio communications. [Washington] U.S. National Institute of Law Enforcement and Criminal Justice, for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1973. 132 p.
"This report presents the results of a one-year technical study of digital data transmission over land-mobile radio channels. Much of the report is devoted to description and analysis of the two major problems of the radio channel--multipath fading and ambient impulsive noise--and their relative effects on error rates for various types of data modulation."

Kenny, Gerard J.
The "national security wiretap": presidential prerogative or judicial responsibility. Southern California law review, v. 45, summer 1972: 888-913.
Thesis of this Comment is that the Fourth Amendment permits no exemption from a warrant requirement for national security wiretaps because "even the most critical of threats to our security cannot justify such a total eclipse of judicial responsibility."

Koehn, Hank E.
Are companies bugged about bugging? Journal of systems management, v. 24, Jan. 1973: 12-13.
"Wiretapping may be illegal, but the equipment isn't. Because it is easy to buy, the data communicator must be concerned about the theft of the data that is entrusted to him to transmit."

Koehn, Hank E.
Privacy, our problem for tomorrow. Journal of systems management, v. 24, July 1973: 8-10.
"A computer cannot invade someone's privacy. If and when there is an invasion or privacy, it is people who are gathering, storing, and misusing data. It is important that we understand the issue."

Kornoff, John Jay.
Police helicopter surveillance and other aided observations: the shrinking reasonable expectation of privacy. California Western law review, v. 11, spring 1975: 505-536.
Comment suggests "that application of the physical presence test of 'plain view' to police helicopter and other aided observations can lead to invasions of our reasonable expectations of privacy, in violation of the fourth amendment."

Lambert, James P.
Lie detectors in the employment context. Louisiana law review, v. 35, spring 1975: 694-703.
Comment discusses "the major legal problems presented by employers' use of the lie detection method as a security measure."

Lambie, William K., Jr.
Electronic surveillance for national security. Journal of police science and administration, v. 3, no. 3, 1975: 346-350.

Land, Thomas.
Privacy vs. the computer revolution. Computers and automation, v. 22, Dec. 1973: 14-16.

Larsen, Kent S., ed.
Privacy, a public concern: a resource document based on the proceedings of a seminar on privacy sponsored by the Domestic Council Committee on the Right of Privacy and the Council of State Governments. [Washington, For sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1975 [i.e. 1976] 183 p.
Partial contents.--Criminal justice information.--Public employee records.--State and local government data banks.--Consumer privacy interests.--Systems cost and the economic impact of implementing privacy legislation.--A strategy for cooperative Federal-state-local privacy programs.

Lateef, A. Bari.
Helicopter patrol in law enforcement--an evaluation. Journal of police science and administration, v. 2, Mar. 1974: 62-65.
Concludes that helicopters are of great utility in law enforcement but that some further evaluation is needed.

The Law, the computer, and you. Bulletin of the American Society for Information Science, v. 1, May 1975: 8-21.
Partial contents.--The legal environment of the information scientist, by J. Farmakides.--Data bases and the lawyer: challenge and enigma, by M. Duggan.--Interaction of antitrust policy and information technology, by B. Bock.--Copyright, photocopying, and computer usage, by B. Linden.--Patent incentives and data processing, by C. Edwards.--The right to privacy, by R. Taeuber.--Computerized information systems as the books, magazines, and journals of the future, by M. Jones.

Lawyers' Committee for Civil Rights Under Law.
Law and disorder, III; state and Federal performance under title I of the Omnibus Crime Control and Safe Streets Act of 1968. [Washington, 1974?] 141 p.
Partial contents.--LEAA and the Federal programs.--Computerized criminal information and intelligence systems.--The hardware industry.

Lewin, Nathan.
Pulling the plug on the FBI's bug; how to stop unjustifiable eavesdropping. New republic, v. 167, July 15, 1972: 12-15.

Lowell, Cyn H.
The corporation's common-law right of privacy: a remedy for the victim of industrial espionage. Corporate practice commentator, v. 14, summer 1972: 156-208.
Reprinted from the 1971 Duke Law Journal, p. 391.
"This article analyze[s] the present legal posture of the industrial espionage victim and suggest[s] one means by which protection might be afforded--that is, through the corporation's common-law right of privacy." Article begins by noting trends which have created a need for corporate privacy protection by the means suggested here.

Lundell, E. Drake. Zientara, Marguerite.
Innocent join the guilty in police computer. New scientist, v. 61, Feb. 28, 1974: 534-535.
Discusses the problems of the FBI's National Crime Information Center, especially lack of privacy safeguards.

Lykken, David T.
Guilty-knowledge test: the right way to use a lie detector. Psychology today, v. 8, Mar. 1975: 56, 58-60.
"Polygraphers now abuse thousands of prospective employees as well as people falsely charged with crime. But psychologists use a fast technique that heads policemen toward the guilty--and assigns guilt to less than one in 10 million innocents."

Mann, Ronni L.
Minimization of wire interception: presearch guidelines and postsearch remedies. Stanford law review, v. 26, June 1974: 1411-1438.
Comment examines the implications of a limiting provision of the 1968 Omnibus Crime Control and Safe Streets Act.

Massachusetts. General Court. Joint Special Committee on the Uses of Modern Electronic Data Processing Systems in the Commonwealth.
The uses of modern electronic data processing systems in the Commonwealth; first interim report. [Boston] 1974. 40 p. (Massachusetts. General Court, 1974. House of Representatives. Documents, no. 5313)

Massey, R. G.
The police patrol car: state of the art. [Washington] National Institute of Law Enforcement and Criminal Justice [for sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1975 [i.e. 1976] 33 p.
At head of title: Law Enforcement Standards Program.
"LESP-RPT-0403.00"
"The objective of this study was to develop an understanding of the vehicles, the accessories and the options that are available for police patrol; the activities for which patrol cars are used by law enforcement agencies; and, the problems encountered by the users in performing the required activities with the available vehicles."

Mathews, David J.
Civilians' claim that Army's data gathering system works a chilling effect on their First Amendment rights held not to be a justiciable controversy absent showing of objective present harm or threat of future harm. Villanova law review, v. 18, Feb. 1973: 479-491.

McChristian, Joseph A.
The role of military intelligence, 1965-1967. Washington, Dept. of the Army [for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1974 [i.e. 1975] 182 p. (Vietnam studies)
Contents.--Introduction.--Combined intelligence.--Combat intelligence.--Intelligence production.--Counterintelligence.--Intelligence support.--Summary.

McGinty, Lawrence.
Fingerprints--the next data in the bank. New scientist, v. 64, Oct. 31, 1974: 320-323.
"Computer systems for identifying people from their fingerprints will soon be installed by police forces throughout the world."

McLaughlin, Marsha Morrow. Vaupel, Suzanne.
Constitutional right of privacy and investigative consumer reports: little brother is watching you. Hastings constitutional law quarterly, v. 2, summer 1975: 773-828.
"The privacy-invading aspects of the investigative credit reporting industry are of growing concern to American consumers. The [student] authors examine abusive practices of the industry as an invasion of the constitutional right of privacy, suggesting judicial remedies for resulting harm. In addition, they evaluate existing controls and propose further legislation to prevent invasions of privacy by investigative consumer reports."

Meisel, Alan.
Political surveillance and the Fourth Amendment. University of Pittsburgh law review, v. 35, fall 1973: 53-71.
"It is the thesis of this article that the fourth amendment to the Constitution provides a foundation for the development of a doctrine for the control of governmentally inspired surveillance." It attempts to design "fourth amendment policies and safeguards against the use by law enforcement officials and other government operatives of surveillance techniques to suppress dissenting ideas, opinions, policies, and personal and social associations."

Metz, Douglas W.
Federal leadership in privacy protection. American Bar Association journal, v. 61, July 1975: 825-829.
"Threats to the right of privacy have been increasing, but with the establishment of the President's Domestic Council Committee on the Right of Privacy, the federal government has signaled its recognition of the threats and its leadership in meeting them through legislation and government policies and practices. Many initiatives have been undertaken by the privacy committee."

The Military after Vietnam: the search for legal controls. Indiana law journal, v. 49, summer 1974: 539-717.
Contents.--Legal inadequacies and doctrinal restraints in controlling the military, by E. Sherman.--The new civil disturbance regulations; the threat of military intervention, by D. Engdahl.--Reflections on the Senate investigation of Army surveillance, by L. Baskir.--Civilian control: new perspectives for new problems, by A. Yarmolinsky.--The control of military organizations in a democratic society: some thoughts concerning the role of social scientists, by M. Garnier.--The new "problem soldier"--dissenter in the ranks, by H. De Nike.--No tunes of glory: America's military in the aftermath of Vietnam, by J. Lovell.

Miller, Arthur R.
The dossier society. University of Illinois law forum, v. 1971, 1971: 154-167.
"What is necessary at this time is the development of a framework for the protection of the public and the superimposition of that framework on information practices at an early date to minimize misuse of an otherwise socially desirable instrument. The problem of striking a balance between democracy and technology has been a frequent and manageable chore in the past and the nation's policy makers should not shrink from the task in this context."

Miller, Arthur Selwyn.
Privacy in the corporate state: a constitutional value of dwindling significance. Journal of public law, v. 22, no. 1, 1973: 3-35.
"Personal privacy is like freedom: both are eighteenth and nineteenth century values of diminishing significance in the modern age--if, indeed, they ever had any substantial basis in social attitudes and behavior. Emphasis on privacy and freedom in law and legal literature comes at precisely the time that the demands of the state for ever increasing amounts of data and the closing of the frontier make their realization, in any reasonably substantial manner, unlikely at best."

Minto, Michael F.
The criminal intelligence squad: strategy and tactics prevention and apprehension. Police chief, v. 42, Feb. 1975: 40-44.
Remarks on "the general attitude, philosophy, and basic problems of those who find themselves working in what could be classified as a criminal intelligence squad."

Missouri. Regional Criminal Justice Information System.
ALERT II: a criminal justice information system. Kansas City, Mo. [1974] 16 p.
"ALERT II is a computerized data base system on crime, crime incidence, wanted or stolen vehicles, wanted persons, known criminals, etc., for a regional area. The data file is continually interrogated by use of remote terminals located as far away as 200 miles."

Morris, Grant.
The computer data bank-privacy controversy revisited: an analysis and an administrative proposal. Catholic University law review, v. 22, spring 1973: 628-650.
Comment examines the increase in numbers of data banks and the existing relevant privacy law, and then proposes "legislative or administrative safeguards which might be established to insure proper protection."

Mortimer, Harold E.
The IRS summons and the duty of confidentiality: a Hobson's choice for bankers--revisited. Banking law journal, v. 92, Sept. 1975: 832-846.
"At present the confidentiality of bank records appears to be in a twilight zone. The developing concept of confidentiality emerging from the cases cited must give a certain pause to the management of a bank, so that--absent judicial or administrative process or the implied or actual consent of the depositor--great caution is exercised in the release of bank records, even to governmental personnel outside of the bank regulatory areas," concludes the author.

Mossman, Keith.
A new dimension of privacy. American Bar Association journal, v. 61, July 1975: 829-833.
"Now that the public has become aroused to the threats to the right of privacy, the new dimension of legal protections must be measured and implemented. There is emerging a general agreement on many legal principles and standards, and the American Bar Association has many committees and groups studying aspects of the problem."

Moster, Clarence R. Pamm, Leonard R.
The Digital Data System launches a new era in data communications. Bell Laboratories record, v. 53, Dec. 1975: 420-426.
"Data can be transmitted much more efficiently in digital form than in analog form. The new DATA-PHONE Digital Service exploits this fact by providing completely digital transmission for data, without any intervening conversion to analog form."

Murphy, John J.
The computer and official retrieval of fugitives. Police chief, v. 42, Dec. 1975: 56-63.
Describes the state of the art of police computerized communications relative to the retrieval of wanted persons.

The National security interest and civil liberties. Harvard law review, v. 85, Apr. 1972: 1130-1326.
An analysis of certain regulatory programs which may be in conflict with political and civil liberties.

Meier, Aryeh.
FBI files: modus inoperandi. Civil liberties, v. 1, summer 1974: 50-58.
Argues for the dismantling of FBI criminal files.

Nelson, Gaylord.
The exposed individual and the secret corporation. Mergers & acquisitions, v. 7, summer 1972: 5-9.
"Senator Nelson (D-Wis.) suggests that the interest of the state and the corporation may be one in eroding individual privacy and in suppressing information about their own activities. Unless this secrecy is ended, he warns, America will move on toward totalitarianism."

Nelson, Gaylord.
"National security" and electronic surveillance: the need for corrective legislation. Intellect, v. 103, Jan. 1975: 230-233.
"Government wiretaps pose a grave danger to the individual's right to privacy and other fundamental constitutional liberties."

Nelson, Gaylord.
Warrantless bugs: the invisible pests. Trial magazine, v. 11, Mar.-Apr. 1975: 64-65, 75.
Senator Nelson presents his outlook on the dangers of wiretapping, suggesting remedies to insure that privacy of citizens will be maintained.

Nesson, Charles R.
Aspects of the executive's power over national security matters: secrecy classifications and foreign intelligence wiretaps. Indiana law journal, v. 49, spring 1974: 399-421.
Article focuses on two executive powers central to the Ellsberg case: the power of national security secrecy classification and the power to use warrantless wiretaps in connection with foreign intelligence. Concludes that it is essential for Congress and the courts to develop checks against them.

New Jersey Electronic Surveillance Act. Rutgers law review, v. 26, spring 1973: 617-646.
Comment examines the New Jersey Wiretapping and Electronic Surveillance Control Act in relation to the minimum standards provided in the Federal Wire Interception and Interception of Oral Communications Act.

Nycum, Susan Hubbell.
Computer abuses raise new legal problems. American Bar Association Journal, v. 61, Apr. 1975: 444-448.

O'Neill, Joseph F.
Tac II: the electronic stakeout. FBI law enforcement bulletin, v. 43, June 1974: 2-6.

O'Reilly, James T.
The Privacy Act of 1974. Columbia, School of Journalism, University of Missouri, 1975. 6 p. (Missouri. University. Freedom of Information Center. Report no. 342)
"The comprehensive Privacy Act of 1974, which goes into effect on Sept. 27, 1975, will have a major impact on the federal government's collection, use and dissemination of information on individual citizens."

O'Toole, George.
Harmonica bugs, cloaks, and silver boxes. Harper's magazine, v. 250, June 1975: 36-39.
Discusses recent strides made in developing more effective and sophisticated eavesdropping devices, describing such items of equipment as the vehicle detention system, the call diverter, the hookswitch bypass, and the harmonica bug among others.

Palme, Jacob.
Software security. Datamation, v. 20, Jan. 1974: 51-55.
"Cryptography, coding, artificial random errors, and keywords are some tools for preventing illegal information access."

Pearce, Harry A.
AWACS to bridge the technological gap. Air University review, v. 23, May-June 1972: 55-61.
Explains the AWACS--a flexible, command, control and surveillance system.

Plate, Thomas.
Wired city: the invasion of the privacy-snatchers. New York, v. 6, July 9, 1973: 28-33.
Investigates the state of legal and illegal wiretaps in New York City.

Platt, George M.
A legislative statement of warrantless earch law: poaching in sacred judicial preserves? Oregon law review, v. 52, winter 1973: 139-154.
Article "analyzes the policy decision in favor of a legislative statement of warrantless search rules" by the Oregon Criminal Law Revision Commission.

Police dossiers--"chilling effect"--First Amendment. Rutgers law review, v. 25, winter-spring 1971: 300-340.
Anderson case contends that records of demonstrations and demonstrators kept by the N.J. police inhibited citizens from exercising their First Amendment rights of speech and assembly. Writer concludes that the most suitable solution to the problem is remedial legislation not judicial resolution.

Potash, Diane Becker.
Maintenance and dissemination of criminal records: a legislative proposal. UCLA law review, v. 19, Apr. 1972: 654-689.
Comment examines and analyzes "the individual's present right to prevent maintenance and disclosure of general police information, and arrest and conviction records" and proposes "safeguards to remedy the inadequacies and uncertainties in the present state of the law."

Powe, Marc B.
Which way for tactical intelligence after Vietnam. Military review, v. 54, Sept. 1974: 48-56.
"Army intelligence was qualitatively better in Vietnam than in previous wars because there was a better intelligence system in support of the tactical forces. This by no means ignores the fact that there were some serious shortcomings in the system. What it says is that improvements in both technology and intelligence concepts created a system more responsive to the tactical commander's needs than in any previous war. Thus, for the future, we should concentrate on exploiting the success of the Vietnam-proven system and correcting the shortcomings."

Powers, Thomas.
The government is watching; is there anything the police don't want to know? Atlantic, v. 230, Oct. 1972: 51-63.
Emphasis on FBI and Army activities against domestic activists.

The Privacy mandate: planning for action; a symposium/workshop, April 2, 23 and 4, 1975. [McLean, Va.] Mitre Corporation, 1975. 102 p.
"Social scientists, economists, and consumers; representatives from Congress, the Administration, and state and local governments; computer scientists and computer industry professionals; and managers from various business and credit communities assembled at the MITRE Conference Center to interact and discuss the implementation of privacy protection." The symposium was jointly sponsored by Mitre and the National Bureau of Standards.

Project Search. Committee on Security and Privacy.
Terminal users agreement for CCH and other criminal justice information. Sacramento, Calif., Project Search, California Crime Technological Research Foundation [1973] 13 p. (Project Search. Technical memorandum no. 5)
"The terminal users agreement discussed in this report creates a legal relationship between an agency which stores and disseminates computerized information and an agency which receives it on-line through a terminal."

Project Search. Latent Fingerprint Subcommittee.
An analysis of automated and semi-automated systems for encoding and searching latent fingerprints. [Sacramento, California Crime Technological Research Foundation] 1974. 69 p. (Project Search. Technical memorandum no. 9)
Surveys "the state-of-the-art in automated and semi-automated methods of searching fingerprints and to evaluate their applicability to searching latent (crime-scene) fingerprints."

Project Search. Latent Fingerprint Subcommittee.
Report on latent fingerprint identification systems. [Sacramento, California Crime Technological Research Foundation] 1974. 188 p. (Project Search. Technical memorandum no. 8)
Surveys, documents, and evaluates existing latent fingerprint systems in use throughout the U.S.

The Protection of privacy: a comparative survey of ten countries by the International Commission of Jurists. International social science journal, v. 24, no. 3, 1972: whole issue.
Contents.--The impact of technological developments on the right to privacy.--The general law relating to privacy in ten countries.--Intrusions into privacy.--Public disclosure of private information.

Pulaski, Charles A., Jr.
Authorizing wiretap applications under title III: another dissent to Giordano and Chavez. University of Pennsylvania law review, v. 123, Apr. 1975: 750-821.
Article examines the Justice Department's procedures and the specifics of the Court's decisions in Giordano and Chavez.

Pyle, Christopher H.
Spies without masters: the Army still watches civilian politics. Civil liberties review, v. 1, summer 1974: 38-49.
Supports passage of a bill to forbid Armed Forces surveillance of any private U.S. citizen.

Ralston, Anthony G.
Computers and democracy. Computers and automation, v. 22, Apr. 1973: 19-22, 40.
"Urban complexity, ecological complexity, political and social complexity require a growing body of administrative law if this planet is going to remain habitable at all. The inevitable result is a gradual restriction on personal freedom in the supposed interests of society at large. The issue...is not whether freedom must be restricted, but in which areas and how much."

Rand Corporation.
Public safety; a bibliography of selected Rand publications. Santa Monica, Calif., 1974. 13 p.
"SB-1048"

Ransom, Harry Howe.
Congress and the intelligence agencies. In Congress against the President. New York, Academy of Political Science, 1975. p. 153-166. (Proceedings, v. 32, no. 1, 1975)
Examines the history of, and issues involved in, the division between Congress and the President of control over, and accountability for, intelligence operations.

Ransom, Harry Howe.
Secret intelligence agencies and Congress. Society, v. 12, Mar.-Apr. 1975: 33-38.
Discusses congressional oversight of intelligence activities.

Ransom, Harry Howe.
Strategic intelligence and foreign policy. World politics, v. 27, Oct. 1974: 131-146.
Reviews 5 books on mostly American intelligence services and concludes with 2 propositions. "1. Intelligence agencies tend to report what they think their leaders want to see or hear. 2. The decision-making leadership sees or hears what it wants, no matter what intelligence is reported."

Raskin, Marcus G. Borosage, Robert L.
National security and official accountability: can we return to government ruled by law? Vital issues, v. 23, Sept. 1973: [1-4]
Addresses the question arising from both the Indochina tragedies and the Watergate affair: "whether the national security institutions can be brought under control by law."

Rogers, Mark J.
Dismissal in civil cases for nondisclosure of surveillance records: potential conflicts with an eavesdropper's constitutional rights. Indiana law journal, v. 48, summer 1973: 662-675.
Comment suggests standards to protect the due process and self-incrimination rights of a civil litigant found to have suppressed evidence of electronic surveillance of the other party.

Roha, Thomas A.
Constitutional law--Bank Secrecy Act--provisions of the act which require the reporting of domestic financial transactions violate the Fourth Amendment's prohibition against unreasonable search and seizure. George Washington law review, v. 42, Oct. 1973: 162-174.

Rosenfeld, Arnold R.
Security and privacy of criminal justice information systems. State government, v. 47, winter 1974: 37-41.
Chairman of the Massachusetts Criminal History Systems Board describes the steps taken to preserve privacy in his state's computerized criminal records.

Ross, Thomas B.
Spying in the United States. Society, v. 12, Mar.-Apr. 1975: 64-70.
The Central Intelligence Agency's "home-front activity had become so extensive by 1964 that the Domestic Operations Division (DOD) had been secretly created to handle it."

Sargent, Francis W.
The National Crime Information Center and Massachusetts. Computers and automation, v. 22, Dec. 1973: 7-10, 20.
The Governor of Massachusetts discussses refusal to tie into the National Crime Information Center.

Saunders, Eric F.
Electronic eavesdropping and the right to privacy. Boston University law review, v. 52, fall 1972: 831-847.
Comment considers majority opinion by Justice White in United States v. White, particularly the "concept of law enforcement's pendant authority to electronically eavesdrop without a warrant, given their constitutional license to employ secret agents." Also compares privacy doctrine in Katz v. United States with the White decision, and proposes an approach to the conflict.

Saxbe, William B.
Organized crime at national levels: wiretapping and electronic surveillance. Police chief, v. 42, Feb. 1975: 20-22.
Discusses the stringent legal controls placed over electronic surveillance.

Schmidt, Wayne W.
A proposal for a statewide law enforcement administrative law council. Journal of police science and administration, v. 2, Sept. 1974: 330-338.
Proposes "the creation of a state law enforcement administration law council in each of the states to promulgate rules governing the conduct and behavior of the police, to guide their activities, and to delineate their discretionary practices."

Schwartz, Barry P.
The recent Swiss-American treaty to render mutual assistance in criminal law enforcement (an application of the Bank Secrecy Act): panacea or placebo? New York University journal of international law & politics, v. 7, spring 1974: 103-136.
Comment considers the problems necessitating the treaty, the treaty's attempted resolution of these difficulties, the possible existence of a constitutional right to financial privacy and the impact of the treaty on it, and alternative solutions the problem.

Schwartz, Herman.
Six years of tapping and bugging. Civil liberties review, v. 1, summer 1974: 26-37.
Details the shortcomings and abuses of government wiretapping and electronic surveillance since its legalization in the 1968 Omnibus Crime Control and Safe Streets Act.

Scoville, Herbert, Jr.
Is espionage necessary for our security? Foreign affairs, v. 54, Apr. 1976: 482-495.
"The recent revelations of abuses by all our intelligence agencies and the multitudinous investigations of the CIA in particular have raised serious questions as to whether the United States can and should continue to maintain a capability to conduct any clandestine operations."

Scoville, Herbert, Jr.
The technology of surveillance. Society, v. 12, Mar.-Apr. 1975: 58-63.
"Technology has not only improved the intelligence data base, but it has done so with increasingly less provocation and fewer political risks."

Shientag, Florence P.
Electronic surveillance, wiretapping: procedures of Federal study commission. Women lawyers journal, v. 61, winter 1975: 6-10, 27.
Member of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance sets forth the authority, goals, and procedures of the Commission.

Siehl, George.
Cloak, dust jacket, and dagger. Library journal, v. 97, Oct. 15, 1972: 3277-3283.
"Recent literature on that 20th-Century phenomenon, the espionage industry."

Smith, Robert Ellis.
Compilation of state laws affecting privacy and personal information. Washington [1975. 12] p.
Monograph to accompany Privacy Journal.

Solmine, Louis P.
Safeguarding the accuracy of FBI records: a review of Menard v. Saxbe and Tarlton v. Saxbe. Cincinnati law review, v. 44, no. 2, 1975: 325-332.
Case note concludes that requiring local law enforcement authorities to forward ultimate disposition of cases to the FBI and permitting claims of inaccuracy to be a reasonable means of aiding reliability.

Sorensen, J. L.
Common sense in computer security. Journal of systems management, v. 23, Apr. 1972: 12-14.
"There are many measures that can be taken to improve computer security. All are costly. But, taking a common sense approach to the problem may help keep the costs down."

Sorkin, Michael.
The FBI's big brother computer. Washington monthly, v. 4, Sept. 1972: 24-30.

St. George, Andrew.
How does it feel to be bugged, watched, followed, hounded and pestered by the C.I.A.? Esquire, v. 83, June 1975: 118-122, 168.
The author relates his experience when he was under surveillance of CIA.

Sefton, John T.
Government access to bank records. Yale law journal, v. 83, June 1974: 1439-1474.
"This note isolates the problem of government access to one type of third party data: checking account records maintained by commercial banks. It is argued that, given the purposes of the Fourth Amendment and the changes which have taken place in the nature of property and privacy, individuals should be able to contest an unreasonable search and seizure of their bank records."

Shattuck, John H. F.
Tilting at the surveillance apparatus. Civil liberties review, v. 1, summer 1974: 59-73.
Describes the successes and failures of legal actions brought by civil liberties groups challenging practices used in surveillance of political groups.

Shattuck, John H. F.
Uncovering surveillance. Trial, v. 11, Jan.-Feb. 1975: 40-41, 48, 50.
Summarizes the issues raised by political surveillance of citizens by the government, briefly listing the major suits which were initiated in response to such surveillance and suggesting possible theoretical approaches for the future handling of surveillance problems.

Sher, Michael S.
A case study in networking. Datamation, v. 20, Mar. 1974: 56-59.
"A university's advanced computation center chose to rely on networking; experiences in using ARPANET resources, and current network economics."

Sheridan, Thomas I., III.
Electronic intelligence gathering and the Omnibus Crime Control and Safe Streets Act of 1968. Fordham law review, v. 44, Nov. 1975: 331-354.
Comment examines the arguments regarding the "applicability of Title III as well as the more important procedural requirements of section 2518" with respect to "electronic surveillance that is intended to produce intelligence information rather than evidence of criminal activity."

Stallings, C. Wayne.
Local information policy: confidentiality and public access. Public administration review, v. 34, May-June 1974: 197-204.
"This article outlines the basic provisions of a model policy which can be adopted by local governments to regulate the collection, storage, use, and dissemination of information in order to protect privacy while assuring that legitimate public access to government records is available."

Stein, Ralph M.
Laird v. Tatum: the Supreme Court and a First Amendment challenge to military surveillance of lawful civilian political activity. In Remarks of Sam J. Ervin, Jr. Congressional record [daily ed.] v. 119, July 18, 1973: S13481-S13489.
Case note discusses Supreme Court decision that justiciability was lacking in a class action complaint against covert internal security activities of the military. The author suggests that Justice Rehnquist may have improperly participated in the decision due to prior involvement in the issue. Reprinted from the HOFSTRA LAW REVIEW.

Stevens, Jean.
Access to personal data files: I. Columbia, School of Journalism, University of Missouri, 1972. 9 p. (Missouri. University. Freedom of Information Center. Report no. 288)
"Considerations of efficiency, economy and security are intruding into the individual citizen's sphere of privacy, as collection, storage and dissemination of personal information increase. This report documents individuals' efforts to gain access to, correct, and control information stored about them by private agencies."

Stevens, Jean.
Access to personal data files: II. Columbia, School of Journalism, University of Missouri, 1972. 16 p. (Missouri. University. Freedom of Information Center. Report no. 291)
"Data accumulated in private agency files, as documented in Report no. 288, is overshadowed by the threat from corresponding government dossiers. One proposed solution is the 'habeas data' concept--access concomitant with the right to know--but so far there are no safeguards, only suggestions, and no laws, only proposals."

Streiff, Charles J.
United States v. United States District for the Eastern District of Michigan: warrantless wiretapping surveillances and the "national security." University of Pittsburgh law review, v. 33, spring 1972: 573-588.
A discussion of the latest developments concerning the "issue of whether the Attorney General...as an agent of the President [can] authorize wiretapping in internal security matters absent judicial sanction."

Symposium on civil liberties policy. Policy studies journal, v. 4, winter 1975: 100-180.
Partial contents.--Restoring the free marketplace: minority access to the media, by F. Lewels.--Children's television programming and censorship, by D. Robinson.--Emerging bases for collective bargaining by college and university faculty, by T. Britton.--The church-state policy process, by D. Fair.--Cruel and unusual punishment: the parameters of the Eighth Amendment, by L. Berkson.--A right of information privacy, by J. Hanus.--The Supreme Court and sexual equality: a case study of factors affecting judicial policy-making, by P. Strum.--Obscenity: denationalization and the conflict of cosmopolitan and local-popular values, by R. Randall.--Assessing the litigative role of ACLU chapters, by S. Halpern.--Civil liberties in revised state constitutions, by A. Sturm and K. Wright.

Szulc, Tad.
The NSA-America's $10 billion Frankenstein. Penthouse, v. 7, Nov. 1975: 55-56, 70, 72, 184, 186, 188, 191, 192, 194-195.
"Our most secret intelligence organization is being devoured by its own technology," claims the author.

Thompson, Patrick A.
Wiretapping--power of United States Attorney-General to authorize wiretapping without judicial sanction. Kentucky law journal, v. 60, fall 1971: 245-252.

Tollett, Kenneth S.
Bugs in the driving dream: the technocratic war against privacy. Howard law journal, v. 17, 1973: 775-796.
Article "categorically condemn[s] electronic surveillance" as an investigative tool.

Turn, Rein. Ware, W. H.
Privacy and security in computer systems. American scientist, v. 63, Mar.-Apr. 1975: 196-203.
"The vulnerability of computerized information has prompted measures to protect both the rights of individual subjects and the confidentiality of research data bases."

U.S. Administrative Office of the United States Courts.
Report on applications for orders authorizing or approving the interception of wire or oral communications; for the period January 1, 1973 to December 31, 1973. Washington [1974?] 191 p.

Consists of "the number of orders and extensions granted or denied during 1973, together with a summary and analysis of the data required by law to be filed with the Administrative Office of the United States Courts by federal and state judges and by federal and state prosecuting officials."

U.S. Commission on CIA Activities Within the United States.
Report to the President. [Washington, 1975] 299 p.
Partial contents.--Summary of the investigation.--The CIA's role and authority.--Supervision and control of the CIA.--Significant areas of investigation.--The CIA's mail intercepts.--Special operations group--"Operation CHAOS".--Involvement of the CIA in improper activities for the White House.--Indicies and files on American citizens.--Allegations concerning the assassination of President Kennedy.

U.S. Congress. House. Committee on Agriculture. Subcommittee on Dept. Operations.
Inspection of farmers' Federal income tax returns by the U.S. Department of Agriculture. Hearings, 93d Cong., 1st sess. Mar. 12 and 28, 1973. Washington, U.S. Govt. Print. Off., 1973. 90 p.
"Serial no. 93-G"

U.S. Congress. House. Committee on Armed Services. Special Subcommittee on Intelligence.
Inquiry into the alleged involvement of the Central Intelligence Agency in the Watergate and Ellsberg matters; report. Washington, U.S. Govt. Print. Off., 1973. 23 p.
At head of title: H.A.S.C. no. 93-25.

U.S. Congress. House. Committee on Banking, Currency and Housing. Subcommittee on Financial Institutions Supervision, Regulation and Insurance.
Bank failures, regulatory reform, financial privacy. Hearings, 94th Cong., 1st sess., on H.R. 8024. Part 2. July 16, 17, and 21, 1975. Washington, U.S. Govt. Print. Off., 1975. 689-1238 p.

U.S. Congress. House. Committee on Banking, Currency and Housing. Subcommittee on Financial Institutions Supervision, Regulation and Insurance.
Bank failures, regulatory reform, financial privacy. Hearings, 94th Cong., 1st sess. on H.R. 8024. Part 1. June 26, July 14, and 15, 1975. Washington, U.S. Govt. Print. Off., 1975. 688 p.

U.S. Congress. House. Committee on Banking, Currency and Housing. Subcommittee on Financial Institutions Supervision, Regulation and Insurance.
Bank failures; regulatory reform; financial privacy. Hearings, 94th Cong., 1st sess., on H.R. 8024. Part 3. Washington, U.S. Govt. Print. Off., 1975. 1241-2234 p.

U.S. Congress. House. Committee on Government Operations.
Federal information systems and plans--implications and issues, part 3. Hearings, 93d Cong., 2d sess. Washington, U.S. Govt. Print. Off., 1974. 811-1214 p.
Hearings held Jan. 29, 31; and Feb. 5, 1974.

U.S. Congress. House. Committee on Government Operations.
Information from farmers' income tax returns and invasion of privacy; sixth report together with additional views. Washington, U.S. Govt. Print. Off., 1973. 25 p. (93d Cong., 1st sess. House. Report no. 93-598)

U.S. Congress. House. Committee on Government Operations.
Privacy Act of 1974; report together with additional views to accompany H.R. 16373. [Washington, U.S. Govt. Print. Off.] 1974. 42 p. (93d Cong., 2d sess. House. Report no. 93-1416)
Recommends legislation "to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies...."

U.S. Congress. House. Committee on Government Operations.
The use of polygraphs and similar devices by Federal agencies; thirteenth report together with separate and dissenting views. Washington, U.S. Govt. Print. Off., 1976. 61 p. (94th Cong., 2d sess. House. Report no. 94-795)
Recommends "that the use of polygraphs and similar devices be discontinued by all Government agencies for all purposes."

U.S. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Access to records. Hearings, 93d Cong., 2d sess., on H.R. 12206 and related bills. Washington, U.S. Govt. Print. Off., 1974. 338 p.
Hearings held Feb. 19...May 16, 1974.
"To amend title 5, United States Code, to provide that persons be apprised of records concerning them which are maintained by government agencies."

U.S. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Executive Orders 11697 and 11709 permitting inspection by the Department of Agriculture of farmers' income tax returns. Hearings, 93d Cong., 1st sess. May 9 and Aug. 3, 1973. Washington, U.S. Govt. Print. Off., 1973. 167 p.

U.S. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Federal information systems and plans--Federal use and development of advanced information technology. Hearings, 93d Cong., 1st sess. Washington, U.S. Govt. Print. Off., 1973. 2 v.
Hearings held Apr. 10, 17 and July 31, 1973.
Parts 1 and 2.

U.S. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Records maintained by government agencies. Hearings, 92d Cong., 2d sess., on H.R. 9527 and related bills. June 22 and 27, 1972. Washington, U.S. Govt. Print. Off., 1972. 232 p.
"To amend Title 5, United States Code, to provide that individuals be apprised or records concerning them which are maintained by government agencies."

U.S. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Sale or distribution of mailing lists by Federal agencies. Hearings, 92d Cong., 2d sess., on H.R. 8903 and related bills. Jan. 13 and 15, 1972. Washington, U.S. Govt. Print. Off., 1972. 362 p.

U.S. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Telephone monitoring practices by Federal agencies. Hearings, 93d Cong., 2d sess. June 11 and 13, 1974. Washington, U.S. Govt. Print. Off., 1974. 293 p.

U.S. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
U.S. Government information policies and practices--problems of Congress in obtaining information from the executive branch. Part 8. Hearings, 92d Cong., 2d sess. Washington, U.S. Govt. Print. Off., 1972. 2939-3312 p.
Hearings held May 12...June 1, 1972.

U.S. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
The use of polygraphs and similar devices by Federal agencies. Hearings, 93d Cong., 2d sess. June 4 and 5, 1974. Washington, U.S. Govt. Print. Off., 1974. 790 p.

U.S. Congress. House. Committee on International Relations.
Middle East agreements and the early warning system in Sinai. Hearings, 94th Cong., 1st sess. Washington, U.S. Govt. Print. Off., 1975. 77 p.
Hearings held Sept. 8...25, 1975.

U.S. Congress. House. Committee on International Relations.
To implement the United Stares proposal for the early-warning system in Sinai; report together with supplemental and additional views on House Joint Resolution 683. Washington, U.S. Govt. Print. Off., 1975. 41 p. (94th Cong., 1st sess. House. Report no. 94-532)

U.S. Congress. House. Committee on Interstate and Foreign Commerce. Special Subcommittee on Investigations.
FCC monitoring of employees' telephones. Hearings, 92d Cong., 2d sess. Washington, U.S. Govt. Print. Off., 1972. 82 p.
Hearings held Mar. 28 and May 16, 1972.
"Serial no. 92-101"

U.S. Congress. House. Committee on Interstate and Foreign Commerce. Special Subcommittee on Investigations.
FCC monitoring of employees' telephones; report. Washington, U.S. Govt. Print. Off., 1973. 77 p. (92d Cong., 2d sess. House. Report no. 92-1632)

U.S. Congress. House. Committee on Post Office and Civil Service.
Census confidentiality/mid-decade sample survey bill; report to accompany H.R. 14153. [Washington, U.S. Govt. Print. Off.] 1972. 27 p. (92d Cong., 2d sess. House. Report no. 92-1288)

U.S. Congress. House. Committee on Post Office and Civil Service.
Census confidentiality/mid-decade sample survey bill; report to accompany H.R. 7762. [Washington, U.S. Govt. Print. Off.] 1973. 25 p. (93d Cong., 1st sess. House. Report no. 93-246)

U.S. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Postal Facilities, Mail, and Labor Management.
Postal Inspection Service's monitoring and control of mail surveillance and mail cover programs. Hearings, 94th Cong., 1st sess. Washington, U.S. Govt. Print. Off., 1975. 238 p.
Hearings held May 6...Nov. 5, 1975.
"Serial no. 94-39"

U.S. Congress. House. Committee on the Judiciary.
Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance; report to accompany H.R. 15173. [Washington, U.S. Govt. Print. Off.] 1974. 5 p. (93d Cong., 2d sess. House. Report no. 93-1343)

U.S. Congress. House. Committee on the Judiciary. Subcommittee No. 4.
Security and privacy of criminal arrest records. Hearings, 92d Cong., 2d sess., on H.R. 13315. Washington, U.S. Govt. Print. Off., 1972. 520 p.
Hearings held Mar. 16...Apr. 26, 1972.
"Serial no. 27"

U.S. Congress. House. Committee on the Judiciary. Subcommittee on Courts, Civil Liberties, and the Administration of Justice.
Surveillance. Hearings, 94th Cong., 1st sess., on the matter of wiretapping, electronic eavesdropping, and other surveillance. Washington, U.S. Govt. Print. Off., 1975. 2 v. (1379 p.)
Hearings held Feb. 6...Sept. 8, 1975.
"Serial no. 26"

U.S. Congress. House. Committee on the Judiciary. Subcommittee on Courts, Civil Liberties, and the Administration of Justice.
Wiretapping and electronic surveillance. Hearings, 93d Cong., 2d sess., on H.R. 1597, H.R. 7773, H.R. 9781, H.R. 9815, H.R. 9973, H.R. 10008, H.R. 10331, H.R. 11629, H.R. 11836, and H.R. 13825. Apr. 24, 26, and 29, 1974. Washington, U.S. Govt. Print. Off., 1974. 275 p.
"Serial no. 41"

U.S. Congress. House. Committee on the Judiciary. Subcommittee on Crime.
Recommendations of the Select Committee on Crime. Hearing, 93d Cong., 2d sess. Mar. 13, 1974. Washington, U.S. Govt. Print. Off., 1975. 39 p.
"Serial no. 64"

U.S. Congress. House. Committee on Ways and Means.
Confidentiality of tax return information. Hearing, 94th Cong., 2d sess. Jan. 28, 1976. Washington, U.S. Govt. Print. Off., 1976. 235 p.

U.S. Congress. House. Select Committee on Intelligence.
Recommendations of the final report; 94th Cong., 2d sess., pursuant to H. Res. 591. Washington, U.S. Govt. Print. Off., 1976. 29 p. (94th Cong., 2d sess. House. Report no. 94-833)

U.S. Congress. House. Select Committee on Intelligence.
U.S. intelligence agencies and activities: committee proceedings. Proceedings, 94th Cong., 1st sess. Part 4. Washington, U.S. Govt. Print. Off., 1976. 1225-1569 p.
[Hearings] held Sept. 10...Nov. 20, 1975.

U.S. Congress. House. Select Committee on Intelligence.
U.S. intelligence agencies and activities: committee proceedings--II. Proceedings, 94th Cong., 2d sess. Part 6. Washington, U.S. Govt. Print. Off., 1976. 2037-2315 p.
Proceedings held Jan. 20...Feb. 10, 1976.

U.S. Congress. House. Select Committee on Intelligence.
U.S. intelligence agencies and activities: domestic intelligence programs. Hearings, 94th Cong., 1st sess. Part 3. Washington, U.S. Govt. Print. Off., 1975. 939-1224 p.
Hearings held Oct. 9...Dec. 10, 1975.
Examines electronic surveillance and the relationship of Federal agencies to local and state police (Oct. 9), DEA's domestic and international intelligence programs (Nov. 13), FBI domestic intelligence programs (Nov. 18), and legal issues involved in domestic intelligence (Dec. 10).

U.S. Congress. House. Select Committee on Intelligence.
U.S. intelligence agencies and activities: intelligence costs and fiscal procedures. Hearings, 94th Cong., 1st sess. Part. 1. Washington, U.S. Govt. Print. Off., 1975. 630 p.

U.S. Congress. Joint Committee on Internal Revenue Taxation. Confidentiality of tax returns. Washington, U.S. Govt. Print. Off., 1975. 44 p.
At head of title: Committee print.

U.S. Congress. Joint Committee on Internal Revenue Taxation. Investigation of the Special Service Staff of the Internal Revenue Service. Washington, U.S. Govt. Print. Off., 1975. 114 p.
At head of title: 94th Cong., 1st sess. Committee print.
"This document deals with the results of the staff investigation on the Special Service Staff, a special unit created in 1969 by the Internal Revenue Service to gather information on so-called 'extremist' organizations and individuals. It also deals with a previous 'Ideological Organizations' project of the Internal Revenue Service that began in 1961, during the Kennedy administration."

U.S. Congress. Senate. Committee on Banking, Housing and Urban Affairs. Subcommittee on Financial Institutions. Amend the Bank Secrecy Act. Hearings, 92d Cong., 2d sess., on S. 3814 and S. 3828. Aug. 11 and 14, 1972. Washington, U.S. Govt. Print. Off., 1972. 337 p.

U.S. Congress. Senate. Committee on Banking, Housing and Urban Affairs. Subcommittee on Financial Institutions. The effect of the Bank Secrecy Act on state laws. Hearings, 93d Cong., 2d sess., on S. 2200. Washington, U.S. Govt. Print. Off., 1974. 213 p.
Hearings held in Los Angeles, Calif.--July 26, 1974; San Francisco, Calif.--July 29, 1974.

U.S. Congress. Senate. Committee on Finance. Subcommittee on Administration of the Internal Revenue Code. Federal tax return privacy. Hearings, 94th Cong., 1st sess. Washington, U.S. Govt. Print. Off., 1975. 308 p.
Hearings held Apr. 21 and 28, 1975.

U.S. Congress. Senate. Committee on Finance. Subcommittee on Administration of the Internal Revenue Code. Federal tax return privacy. Hearings, 94th Cong., 2d sess. Apr. 21 and 28, 1975, and Jan. 23, 1976. Part 2. Washington, U.S. Govt. Print. Off., 1976. 129 p.

U.S. Congress. Senate. Committee on Foreign Relations. CIA foreign and domestic activities. Hearing, 94th Cong., 1st sess. Jan. 22, 1975. Washington, U.S. Govt. Print. Off., 1975. 39 p.

U.S. Congress. Senate. Committee on Foreign Relations.
Early warning system in Sinai. Hearings, 94th Cong., 1st sess. Oct. 6 and 7, 1975. Washington, U.S. Govt. Print. Off., 1975. 264 p.

U.S. Congress. Senate. Committee on Foreign Relations.
Early warning system in Sinai; report together with individual views to accompany S. J. Res. 138. [Washington, U.S. Govt. Print. Off.] 1975. 20 p. (94th Cong., 1st sess. Senate. Report no. 94-415)

U.S. Congress. Senate. Committee on Foreign Relations. Subcommittee on Surveillance.
Warrantless wiretapping and electronic surveillance; report. Washington, U.S. Govt. Print. Off., 1975. 11 p.
At head of title: 94th Cong., 1st sess. Committee print.
Recommends extensive reform "for all electronic surveillance activities carried out in the United States for military security, national defense or foreign intelligence gathering purposes."

U.S. Congress. Senate. Committee on Government Operations.
Oversight of U.S. Government intelligence functions. Hearings, 94th Cong., 2d sess., on S. 317, S. 189, S. Con. Res. 4, S. 2893 [and] S. 2865. Washington, U.S. Govt. Print. Off., 1976. 535 p.
Hearings held Jan. 21...Feb. 6, 1976.

U.S. Congress. Senate. Committee on Government Operations. Ad Hoc Subcommittee on Privacy and Information Systems.
Privacy; the collection, use, and computerization of personal data. Joint hearings before the Ad Hoc Subcommittee on Privacy and Information Systems of the Committee on Government Operations and the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, 93d Cong., 2d sess., on S. 3418, S. 3633, S. 3116, S. 2810 [and] S. 2542. June 18-20, 1974. Washington, U.S. Govt. Print. Off., 1974. 2 v. (2335 p.)

U.S. Congress. Senate. Committee on Government Operations. Subcommittee on Intergovernmental Relations.
Legislative proposals to strengthen congressional oversight of the Nation's intelligence agencies. Hearings, 93d Cong., 2d sess., on S. 4019, S. 2738, S. Res. 419, and S. 1547. Dec. 9 and 10, 1974. Washington, U.S. Govt. Print. Off., 1975. 205 p.

U.S. Congress. Senate. Committee on the Judiciary.
Protecting privacy and the rights of Federal employees; report to accompany S. 1688. [Washington, U.S. Govt. Print. Off.] 1974. 48 p. (93d Cong., 1st sess. Senate. Report no. 93-724)

"The purpose of the bill is to prohibit indiscriminate executive branch requirements that employees and, in certain instances, applicants for Government employment disclose their race, religion, or national origin; attend Government-sponsored meetings and lectures or participate in outside activities unrelated to their employment; report on their outside activities or undertakings unrelated to their work; submit to questioning about their religion, personal relationships or sexual attitudes through interviews, psychological tests, or polygraphs; support political candidates or attend political meetings. The bill would make it illegal to coerce an employee to buy bonds or make charitable contributions."

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure.
IRS disclosure. Hearings, 93d Cong., 2d sess. Washington, U.S. Govt. Print. Off., 1974. 294 p.
Hearings held Apr. 1 and July 31, 1974.
Hearings into IRS compliance with the Freedom of Information Act.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure.
Warrantless wiretapping. Hearings, 92d Cong., 2d sess. June 29, 1972. Washington, U.S. Govt. Print. Off., 1973. 221 p.
Hearings provide various views of the impact and significance of the Supreme Court decision in the Keith Case (United States v. United States District Court for the Eastern District of Michigan).

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure.
Warrantless wiretapping and electronic surveillance--1974. Joint hearings, 93d Cong., 2d sess. Washington, U.S. Govt. Print. Off., 1974. 519 p.
Hearings held Apr. 3...May 23, 1974.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Army surveillance of civilians: a documentary analysis. Washington, U.S. Govt. Print. Off., 1972. 97 p.
At head of title: 92d Cong., 2d sess. Committee print.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Criminal justice data banks--1974. Hearings, 93d Cong., on S. 2542, S. 2810, S. 2963, and S. 2964. Volume II--appendix. Washington, U.S. Govt. Print. Off., 1974. 1149 p.
Hearings held Mar. 5...14, 1974.
Bibliography: p. 1111-1149.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Criminal justice data banks--1974. Hearings, 93d Cong., on S. 2542, S. 2810, S. 2963, and S. 2964. Volume I. Washington, U.S. Govt. Print. Off., 1974. 733 p.
Hearings held Mar. 5...14, 1974.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Criminal Justice Information and Protection of Privacy Act of 1975. Hearings, 94th Cong., 1st sess., on S. 2008, S. 1427, and S. 1428. July 15-16, 1975. Washington, U.S. Govt. Print. Off., 1975. 311 p.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Federal data banks and constitutional rights; a study of data systems on individuals maintained by agencies of the United States Government. 93d Cong., 2d sess. Washington, U.S. Govt. Print. Off., 1974. 6 v. (3527 p.)
At head of title: Committee print.
Partial contents.--v. 1. Civil Service Commission.--Department of Agriculture.--Department of Commerce.--v. 2. Department of Defense.--v. 3. Department of Health, Education, and Welfare.--Department of Housing and Urban Development.--v. 4. Department of the Interior.--Department of Justice.--Department of Labor.--Department of State.--Department of Transportation.--v. 5. Department of the Treasury.--v. 6. U.S. Postal Service.--White House.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Federal data banks, computers and the Bill of Rights. Hearings, 92d Cong., 1st sess. Washington, U.S. Govt. Print. Off., 1971. 1047-2164 p.
Hearings held Feb. 23...Mar. 17, 1971.
Part II--relating to Departments of Army, Defense, and Justice.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Military surveillance. Hearings, 93d Cong., 2d sess., on S. 2318. Apr. 9 and 10, 1974. Washington, U.S. Govt. Print. Off., 1974. 397 p.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Military surveillance of civilian politics; report. Washington, U.S. Govt. Print. Off., 1973. 150 p.
At head of title: 93d Cong., 1st sess. Committee print.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Political intelligence in the Internal Revenue Service: the Special Service Staff; a documentary analysis. Washington, U.S. Govt. Print. Off., 1974. 344 p.
At head of title: Committee print.
"During the years 1969 through 1973 the Internal Revenue Service maintained a special political surveillance unit known as the Special Service Staff, the purpose of which was the collection of 'all available information on organizations and individuals promoting extremists' views on philosophies.'"

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Privacy, polygraphs, and employment; a study. Washington, U.S. Govt. Print. Off., 1974. 18 p.
At head of title: 93d Cong., 2d sess. Committee print.
Explores use of the polygraph to check into employee suitability in government and private business, focusing on the constitutional issue of individual rights raised by the practice.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures.
Electronic surveillance for national security purposes. Hearings, 93d Cong., 2d sess., on S. 2820, S. 3440, and S. 4062. Oct. 1, 2, and 3, 1974. Washington, U.S. Govt. Print. Off., 1975. 577 p.

U.S. Congress. Senate. Select Committee on Presidential Campaign Activities.
Draft of final report. Washington, U.S. Govt. Print. Off., 1974. 3 v.
Contents.--Watergate break-in and coverup.--Campaign practices.--Use of incumbency responsiveness program.--Campaign financing.--Milk fund.--Humphrey campaign financing.--Mills campaign financing.--Hughes-Rebozo investigation and related matters.--The Select Committee in court.--The Select Committee's use of computer technology.--Individual views of Senators of the Select Committee.
At head of title: 93d Cong., 2d sess. Committee print.

U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities.
Intelligence activities, Senate Resolution 21. Hearings, 94th Cong., 1st sess. Oct. 2, 1975. Washington, U.S. Govt. Print. Off., 1976. 124 p.
Vol. 3--Internal Revenue Service.

U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities.
Intelligence activities, Senate Resolution 21. Hearings, 94th Cong., 1st sess. Sept. 23-25, 1975. Washington, U.S. Govt. Print. Off., 1976. 403 p.
Vol. 2--Huston plan.

U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities.
Intelligence activities, Senate Resolution 21. Hearings, 94th Cong., 1st sess. Washington, U.S. Govt. Print. Off., 1976. 1000 p.
Volume 6--Federal Bureau of Investigation.
Hearings held Nov. 18...11, 1975.

U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities.
Intelligence activities, Senate Resolution 21. Hearings, 94th Cong., 1st sess. Oct. 29 and Nov. 6, 1975. Washington, U.S. Govt. Print. Off., 1976. 165 p.
Vol. 5--The National Security Agency and Fourth Amendment rights.

U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities.
Intelligence activities, Senate Resolution 21. Hearings, 94th Cong., 1st sess. Oct. 21, 22, and 24, 1975. Washington, U.S. Govt. Print. Off., 1976. 260 p.
Vol. 4--Mail opening.

U.S. Dept. of Health, Education, and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems.
Records, computers and the rights of citizens. Washington, For sale by the Supt. of Docs., U.S. Govt. Print. Off., 1973. 346 p. (U.S. Dept. of Health, Education, and Welfare. DHEW publication no. (OS) 73-94)
Report of a committee of "experienced and concerned citizens" appointed by HEW which "assessed the impact of computer-based record keeping on private and public matters and recommended safeguards against its potentially adverse effects"; particular attention was focused on the dangers of the movement to use the social security number as an "all-purpose personal identifier" and on the "need to insulate statistical-reporting and research data from compulsory legal process."
Bibliography: p. 298-330.

U.S. Dept. of Justice.
Criminal justice information systems. Federal register, v. 40, May 20, 1975: 22113-22119.
Sets forth "regulations governing the dissemination of criminal record and criminal history information and includes a commentary on selective sections as an appendix. Its purpose is to afford greater protection of the privacy of individuals who may be included in the records of the Federal Bureau of Investigation, criminal justice agencies receiving funds directly or indirectly from the Law Enforcement Assistance Administration, and interstate, state or local criminal justice agencies exchanging records with the FBI or these federally funded systems."

U.S. Drug Enforcement Administration. Special Programs Division.
Drug abuse warning network (DAWN I analysis). Washington, 1973. 137 p.
Presents interim report on the Drug Abuse Warning Network (DAWN I), a government data base whose information is gathered from hospitals emergency departments, medical examiners, student health centers, and crisis intervention centers.

U.S. Federal Bureau of Investigation.
The science of fingerprints; classification and uses. Washington, For sale by the Supt. of Docs., U.S. Govt. Print. Off. [1973] 198 p.
Partial contents.--The Identification Division of the FBI.--Types of patterns and their interpretation.--Filing sequence.--Searching and referencing.--The National Crime Information Center fingerprint classification system.--Establishment of a local fingerprint identification bureau.--Powdering and latent impressions.

U.S. Federal Bureau of Investigation.
Uniform crime reports for the United States, 1972. Washington, For sale by the Supt. of Docs., U.S. Govt. Print. Off., 1973. 272 p.

U.S. General Accounting Office.
Development of a nationwide criminal data exchange system--need to determine cost and improve reporting, Department of Justice; report to the Congress by the Comptroller General of the United States. [Washington] 1973. 20 p.

U.S. General Accounting Office.
Development of the computerized criminal history information system. Washington, 1974. 10 l.
"B-171019, Mar. 1, 1974"

U.S. General Accounting Office.
Difficulties of assessing results of Law Enforcement Assistance Administration projects to reduce crime, Department of Justice; report to the Congress by the Comptroller General of the United States. [Washington] 1974. 71 p.
"B-171019, Mar. 19, 1974"

U.S. General Accounting Office.
FBI domestic intelligence operations--their purpose and scope: issues that need to be resolved; report to the House Committee on the Judiciary by the Comptroller General of the United States. [Washington] 1976. 232 p.
"GGD-76-50, Feb. 24, 1976"
"The FBI's authority to carry out domestic intelligence investigations is unclear. Legislation is needed. Investigations are too broad in terms of the number of people investigated and scope of investigations. Legislation is needed. Investigations are generally passive in that information is gathered from other sources. But they are all encompassing. Questionable techniques were used infrequently, but legislation is needed limiting their future use. The FBI adequately controlled dissemination of investigative information, but has not adequately examined its procedures for maintaining such data. The Attorney General should limit retention of investigation data. Neither the Justice Department nor the Congress exercised adequate control and oversight over FBI domestic intelligence operations. Legislation is needed."

U.S. General Accounting Office.
Personnel security investigations: inconsistent standards and procedures, Civil Service Commission. [Washington] 1974. 18 p.
"B-132376, Dec. 2, 1974"
Recommends that, due to extensive differences among executive agencies in the object, scope, and use of loyalty-security investigations, this function be centralized in two agencies, one for defense employment and one for civilian employment.

U.S. Law Enforcement Assistance Administration.
1972 directory of automated criminal justice information systems. [Washington] 1972. 1 v. (various pagings)
"This directory contains an indexed listing of the automated criminal justice information systems used by police, courts, corrections and other agencies. For each jurisdiction covered, the listing describes briefly criminal justice information systems which are operational or being developed, who is doing the work and the current status of the systems."

U.S. Law Enforcement Assistance Administration. Office of General Counsel.
Compendium of state laws governing the privacy and security of criminal justice information. Washington, 1975. 1 v. (various pagings)

U.S. Library of Congress. American Law Division.
Internal security manual, revised to July 1973. Provisions of Federal statutes, executive orders, and congressional resolutions relating to the internal security of the United States. Prepared...at the request of the Subcommittee to Investigate the Administration of the Internal Security Act and Other Internal Security Laws of the Committee on the Judiciary, United States Senate. Washington, U.S. Govt. Print. Off., 1974. 2 v. (1017 p.)
At head of title: 93d Cong., 2d sess. Committee print.
"Revision of Senate Document no. 126, 86th Congress, 2d session."

U.S. Library of Congress. Foreign Affairs Division.
Soviet intelligence and security services, 1964-70: a selected bibliography of Soviet publications, with some additional titles from other sources. Prepared by the Congressional Research Service, Library of Congress, at the request of and based on materials provided by the Subcommittee to Investigate the Administration of the Internal Security Act and Other Internal Security Laws of the Committee on the Judiciary, United States Senate. Washington, U.S. Govt. Print. Off., 1972. 289 p.
At head of title: 92d Cong., 1st sess. Committee print.

U.S. National Bureau of Standards.
Computer security guidelines for implementing the Privacy Act of 1974. [Washington, For sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1975. 20 p. (Federal information processing standards publication. FIPS pub. 41)
"A wide variety of technical and related procedural safeguards are described. These fall into three broad categories: Physical security, information management practices, and computer system/network security controls. As each organization processing personal data has unique characteristics, specific organizations should draw upon the material provided in order to select a well-balanced combination of safeguards which meets their particular requirements."

U.S. Office of the Federal Register.
Protecting your right to privacy. [Washington, 1976] 737 p.
Lists systems of records kept by Federal agencies, reprints agency rules governing their use under the Privacy Act, and includes several research aids.

United States v. Cafero; United States Court of Appeals for the Third Circuit--nos. 72-1577 and 72-1578. In Remarks of John L. McClellan. Congressional record [daily ed.] v. 119, Feb. 21, 1973: S3040-S3044.
Text of opinion of Circuit Judge Ruggero Aldisert in United States v. Cafero, which upholds title III of the Omnibus Crime Control and Safe Streets Act of 1968.

VanZile, Philip T., III.
The right of privacy: actions in intrusion for electronic eavesdrop and wiretap. Journal of urban law, v. 51, Aug. 1973: 79-93.
Comment explores tort law in the area of actions for privacy intrusions through wiretapping and electronic eavesdropping. The author also examines the question in the context of news gathering by reporters.

Virginia. Advisory Legislative Council.
Computer privacy and security; report to the Governor and the General Assembly of Virginia. Richmond, Commonwealth of Virginia, Dept. of Purchases and Supply, 1975. 15 p. (Virginia. General Assembly, 1975. House of Delegates. Document no. 18)

The Voiceprint dilemma: should voices be seen and not heard? Maryland law review, v. 35, no. 2, 1975: 267-296.

Note examines "the theoretical basis and current scientific status of the voiceprint technique before discussing the technique's legal history and attempting to isolate the proper test for its admission into evidence and the proper result thereunder."

Voiceprint identification. Georgetown law journal, v. 61, Feb. 1973: 703-745.

Comment examines "the voiceprint identification process by focusing on the scientific controversy surrounding the reliability of spectrographic identification," reviews cases which have had voiceprint use rulings, and analyzes "the substantial evidentiary and constitutional questions presented by the admissibility of voiceprint evidence."

Voysey, Hedley. Hanlon, Joseph.

Data bank control--some day. New scientist, v. 69, Jan. 1, 1976: 26-27.

"'The time has come when those who use computers to handle personal information, no matter how responsible they are, can no longer remain the sole judges of whether their own systems adequately safeguard privacy,' according to the [British Government's] Computers and Privacy white paper, [Cmnd 6353] just published."

Ware, Willis H.

Records, computers, and the rights of citizens. Datamation, v. 19, Sept. 1973: 112-114.

"Citizens should be able to control personal information kept on them in government files."

Weissman, Anita S.

Voiceprints and the defense. New England law review, v. 10, fall 1974: 25-83.

Article discusses the use of voiceprints as evidence in criminal cases. Controls on the use of recorded material in the courts are discussed.

Westin, Alan F.

Databanks in a free society: a summary of the Project on Computer Databanks. Computers and automation, v. 22, Jan. 1973: 18-22.

"Our task is to see that appropriate safeguards for the individual's rights to privacy, confidentiality, and due process, are embedded in every major record system in the nation."

Westin, Alan F.
Databanks in a free society: a summary of the project on computer databanks. Law and computer technology, v. 6, July-Aug. 1973: 93-104.
Article based on a 3 year study of data banks in the United States.

Westin, Alan F.
The problem of privacy and security with computerized data collection. Conference Board record, v. 11, Mar. 1974: 31-34.
Discusses the problem of privacy and security with computerized personal records and the implications for management.

Wiesner, Jerome B.
The information revolution--and the Bill of Rights. Law and computer technology, v. 5, Mar.-Apr. 1972: 40-46.
"The present capabilities in information collection have already led to clear-cut infringements of citizens rights. In fact, even without technological assistance, there have been serious violations of the constitutional protections by many agencies of the government and by many private organizations. Furthermore, the awareness of security dossiers has inhibited many people in their political activities."

Williams, David L.
Wiretap of domestic subversives without warrant but authorized by Attorney General for national security reasons held violative of Fourth Amendment. Villanova law review, v. 17, Feb. 1972: 545-559.
Case note describes decision of Sixth Circuit Court of Appeals which held that domestic wiretaps were illegal unless they complied with the Fourth Amendment and that their transcripts must be made available to the defendant "without requiring a judge's in camera inspection to determine the material's relevance."

Witt, Barbara.
Computers and data banks in Government: a selective bibliography. Monticello, Ill., 1973. 20 p. (Council of Planning Librarians. Exchange bibliography 487)

APPENDIX D.2

SURVEILLANCE, PRIVACY, AND RELATED ITEMS

MARC DEVELOPMENT OFFICE
INFORMATION SYSTEMS OFFICE

JULY 1976

Ackroyd, James E.
The investigator; a practical guide to private detection [by] James E. Ackroyd. [London] Muller [1974]
125 p. 22 cm. £2.35
HV8081 .A25 1974

Akin, Richard H.
The private investigator's basic manual of procedure / by Richard H. Akin. Springfield, Ill. : Thomas, c1976.
p. cm.
Includes bibliographical references and index.
HV8073 .A56

American Bar Association. Special Committee on Standards for the Administration of Criminal Justice.
Standards relating to electronic surveillance; proposed final draft. Recommended by the Special Committee on Standards for the Administration of Criminal Justice and the Advisory Committee on the Police Function. A. Robert Blakey, reporter. [New York, Institute of Judicial Administration, Secretariat] 1971.
27 p. 23 cm.
At head of title: American Bar Association Project on Standards for Criminal Justice.
KF8670.Z9 A4

Altman, Irwin.
The environment and social behavior : privacy, personal space, territory, crowding / Irwin Altman ; Lawrence S. Wrightsman, consulting editor. Monterey, Calif. : Brooks/Cole Pub. Co., c1975.
xi, 256 p. : ill. ; 24 cm.
Includes index. Bibliography: p. 221-237.
HM291 .A489

Approaches to privacy and security in computer systems; proceedings of a conference held at the National Bureau of Standards, March 4-5, 1974. Clark R. Penninger, editor. [Washington] National Bureau of Standards; [for sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1974.
xi, 71 p. illus. 26 cm. (National Bureau of Standards special publication 404)
Includes bibliographical references.
QC100 .U57 no. 404 JC599.U5
389/.08 s 323.44
74-16117

Arons, Harry.
Hypnosis in criminal investigation. With forewords by William S. Kroger, Dewey Kelley [and] James P. Devine. Springfield, Ill., C. C. Thomas [1967]
xxvii, 211 p. 24 cm.
Includes bibliographical references.
RA1171 .A7

Asch, Sidney H.
Police authority and the rights of the individual [by] Sidney H. Asch. New York, Arco [1967]
126 p. 23 cm. (Know your law)
"Notes": p. 121-123.
KF9625 .A98

Asch, Sidney H.
Police authority and the rights of the individual [by] Sidney H. Asch. [2d ed.] New York, Arco [1968]
viii, 146 p. 23 cm. (Know your law)
Bibliographical references included in "Notes" (p. 135-142)
KF9625 .A98 1968

Asch, Sidney H.
Police authority and the rights of the individual [by] Sidney H. Asch. [3d ed.] New York, Arco [1971]
vi, 170 p. 23 cm. (Know your law) $4.95
Includes bibliographical references.
KF9625 .A98 1971

Association of the Bar of the City of New York. Committee on Federal Legislation.
Government databanks and rights of individuals, H.R. 16373 and S. 3418 / by the Committee on Federal Legislation. New York : Association of the Bar of the City of New York, 1974.
52 p. ; 23 cm. (Federal legislation report ; no. 74-9)
Caption title. Includes bibliographical references.
KF5752.5 .A7

Bacon, Michael David.
Data transmission [by] M. D. Bacon and G. M. Bull. London, Macdonald and Co.; New York, American Elsevier, 1973.
[9], 135 p. illus. 23 cm. (Computer monographs, 20) £2.50
Includes index. Bibliography: p. 132-133.
TK5102.5 .B29

Baer, Walter S.
Interactive television: prospects for two-way services on cable [by] Walter S. Baer. Santa Monica, Calif., Rand, 1971.
xvii, 88 p. 28 cm. (Rand Corporation. R-888-MF)
"A report prepared under a grant from the John and Mary A. Markle Foundation."
Includes bibliographical references.
AS36 .R3 R-888 TK6675

Barefoot, J. Kirk.
The polygraph story : dedicated to man's right to verify the truth / J. Kirk Barefoot, editor ; authors, Stanley Abrams ... [et al.] ; contributors, Richard O. Arther ... [et al.]. Rev. 3d printing. [Hollywood, Calif.] : American Polygraph Association, 1974.
34 p. ; 29 cm.
Published in 1973 under title: The polygraph technique. Includes bibliographies.
KF9666.Z9 B3 1974
347/.73/62
75-316704

Barefoot, J. Kirk.
Undercover investigation / by J. Kirk Barefoot ; with a foreword by V. A. Leonard. Springfield, Ill. : Thomas, [1975]
xii, 87 p. : ill. ; 24 cm.
Includes index. Bibliography: p. 84.
HV8080.U5 B37

Beall, James R.
Helicopter utilization in municipal law enforcement; administrative considerations, by James R. Beall and Robert E. Downing. Springfield, Ill., Thomas [c1972]
ix, 80 p. 24 cm.
Bibliography: p. 75.
HV8080.A3 B4

Becker, Hal B.
Functional analysis of information networks: a structured approach to the data communications environment [by] Hal B. Becker. New York, Wiley [1973]
xiii, 281 p. illus. 23 cm. (Business data processing)
"A Wiley-Interscience publication."
Bibliography: p. 269-271.
TK5102.5 .B35

Bennett, John Tuson.
Invasions of privacy [by] John Bennett. [Melbourne, Victorian Council for Civil Liberties?] 1968.
12 p. 34 cm. unpriced
Cover title. At head of title: First Australian Convention, Councils for Civil Liberties, Sydney, 1968. Bibliography: p. [3] of cover.
LAW

Bergier, Jacques, 1912-
Secret armies : the growth of corporate and industrial espionage / by Jacques Bergier ; translated from the French by Harold J. Salemson. Indianapolis : Bobbs-Merrill, c1975.
268 p. ; 24 cm.
Translation of the author's three separate works originally published under titles: L'espionnage industriel, L'espionnage scientifique, and L'espionnage strategique.
HD38 .B386 1975

Blackstock, Paul W.
Intelligence, espionage, counterespionage, and covert operations : a guide to information sources / Paul W. Blackstock, Frank L. Schaf, Jr. Detroit : Gale Research Co., 1975.
p. cm. (International relations information guide series ; v. 2)
Includes index. Bibliography: p.
Z6724.I7 B55 UB250

Bloch, Peter B., 1940-
Managing criminal investigations / by Peter B. Bloch, Donald R. Weidman. Washington : U.S. Dept. of Justice, Law Enforcement Administration, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal : for sale by Supt. of Docs., U.S. Govt. Print. Off., 1975.
xii, 145 p. : forms ; 26 cm.
Cover title: Prescriptive package : managing criminal investigations. Includes bibliographical references.
HV8073 .B57
364.12
75-619207

Breckenridge, Adam Carlyle, 1916-
The right to privacy. Lincoln, University of Nebraska Press [1970]
155 p. 21 cm. 5.75
Bibliographical footnotes.
KF1262 .Z9B7

British Columbia. Royal Commission of Inquiry into Invasion of Privacy.
Report. [Victoria, 1967]
56 l. 36 cm. 1.00
Cover title. Inquiry pursuant to the Public Inquiries act. c. 315, R.S.B.C. 1960, and Order in Council no. 1, Jan. 3, 1967.
Commissioner: R. A. Sargent.
JC599.C2 B7

British Computer Society. Privacy and Public Welfare Committee.
Questionnaire on privacy and the computer : a technical project of the Privacy and Public Welfare Committee of the British Computer Society / compiled by a working party of the Privacy & Public Welfare Committee. [s.l. : s.n., 1972?] ([London : British Computer Society])
61 p. ; 30 cm.
Cover title.
JC599.G7 B75 1972

British Computer Society. Privacy Committee.
Submission of evidence to the Committee on Privacy. London, British Computer Society (Committee on Privacy), 1971.
[6], 25 leaves. 30 cm.
JC599.G7 B75 1971

Brown, Robert Michael, 1943-
The electronic invasion / Robert M. Brown. Rev. 2d ed. Rochelle Park, N.J. : Hayden Book Co., [1975]
180 p. : ill. ; 21 cm.
Includes index.
TK7882.E2 B75 1975

Burton, Alan.
Police telecommunications. With a foreword by George K. Burton. Illus. by Rod Carpenter. Springfield, Ill., Thomas [1973]
xi, 438 p. illus. 24 cm.
Bibliography: p. 428-430.
HV7936.C8 B8

Bushkin, Arthur A., 1943-
The Privacy act of 1974 : a reference manual for compliance / Arthur A. Bushkin, Samuel I. Schaen. McLean, Va. : System Development Corp., c1975.
p. cm. (Technical memorandum, TM series)
"Appendix B: Public law 93-579: the Privacy act of 1974": p. Includes index.
Bibliography: p.
KF1262 .B8

Butler, Henry E.
Legal aspects of student records [by] Henry E. Butler, Jr., K. D. Moran [and] Floyd A. Vanderpool, Jr. Topeka, National Organization on Legal Problems of Education, 1972.
62 p. 23 cm. (NOLPE monograph series, no. 5) (ERIC/CEM state-of-the-knowledge series, no. 12)
"Commissioned by ERIC Clearinghouse on Educational Management." Includes bibliographical references.
KF4150.Z9 B87
344/.73/0793
73-156977

California. Legislature. Assembly. Committee on Efficiency and Cost Control.
Assembly bill 2656, Protection of individual rights in a computer environment; hearing. December 21, 1973. [Sacramento, 1973]
34[l. 29 cm.
Cover title. "ECC 73-16."
JC599.U52 C33 1973

California. Legislature. Assembly. Committee on Efficiency and Cost Control.
State consolidated data centers: computer privacy and security. Hearing. [Sacramento] 1973-
v. 28 cm.
Cover title. "ECC 73-7." Hearings held Mar. 27- 1973.
JK8749.A8 C324 1973

Calkins, Clinch.
Spy overhead: the story of industrial espionage. New York, Arno, 1971 [c1965]
363 p. 23 cm. (American labor: from conspiracy to collective bargaining)
HD6508 .C17 1971

Carroll, John Millar.
Confidential information sources, public & private / John M. Carroll. 1st ed. Los Angeles : Security World Pub. Co., 1975.
xv, 335 p. : ill. ; 24 cm.
Includes index. Bibliography: p. 315-318.
JC599.U5 C356

Carroll, John Millar.
The third listener; personal electronic espionage, by John M. Carroll. [1st ed.] New York, Dutton, 1969.
178 p. illus. 22 cm. 4.95
TK7882.E2 C3

Cederbaums, Juris.
Wiretapping and electronic eavesdropping: the law and its implications; a comparative study. [New York, Criminal Law Education and Research Center, New York University; distribution by F. B. Rothman, South Hackensack, N.J., 1969]
77 p. illus. 25 cm. (New York University. Criminal Law Education and Research Center. Monograph series, v. 2)
Includes bibliographical references.
KF9670 .Z9C43

Chief Justice Earl Warren Conference on Advocacy in the United States, Cambridge, Mass., 1974.
Privacy in a free society : final report : annual Chief Justice Earl Warren Conference on Advocacy in the United States, June 7-8, 1974 / sponsored by the Roscoe Pound-American Trial Lawyers Foundation. [Cambridge, Mass. : Roscoe Pound-American Trial Lawyers Foundation, 1974]
104 p. : port. ; 25 cm.
Includes bibliographical references.
KF1262.A75 C45 1974

Chu, Wesley W., comp.
Advances in computer communications [by] Wesley W. Chu. [Dedham, Mass., Artech House, 1974]
xv, 490 p. illus. 29 cm. (Modern frontiers in applied science)
"An Artech House reprint volume." Includes bibliographical references.
TK5102.5 .C48
001.6/44/04
ISBN 0890060290
74-77722

Coghill, Mary Ann.
The lie detector in employment: an examination of some of the problems, by Mary Ann Coghill, with additions by Elaine F. Gruenfeld. Rev. Ithaca, N.Y., New York State School of Industrial and Labor Relations, Cornell University, 1973.
35 p. 28 cm. (Key issues series, no. 2)
Bibliography: p. 20-22.
HV8078 .C63 1973

Commission studies. Washington : National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, 1976.
p. cm. (Supporting materials for the Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance)
Consists of studies prepared for the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance.
KF9670.A75 C6

Committee of One Hundred, London. Hampstead Group.
Mail interception and telephone tapping in Britain. Brighton, Attila Publications; [distributed by] Smoothie Publications, 1973.
[4], 12 p. 26 cm. £0.15
Includes bibliographical references.
JC599.G7 C65 1973

Committee of One Hundred, London. Hampstead Group.
Mail interception and telephone tapping in Britain. 3rd ed. Brighton : Smoothie Publications, 1974.
[2], 11 p. ; 30 cm.
JC599.G7 C65 1974

Computer abuse. New York : Practising Law Institute, c1975.
208 p. (p. 207-208 blank) ; 22 cm.
(Litigation course handbook series ; no. 77)
"H4-3823." "Prepared for distribution at the computer abuse program, November-December 1975." Includes the Privacy act of 1974 and Title 5, Government organization and employees, of the Freedom of information act.
Includes bibliographical references and index.
KF390.5.C6 C6

Conference on American Freedom, Washington, D.C., 1973.
Papers from the Conference on American Freedom [about] press, privacy, religion, speech. [n.p., 1973]
63 p. 28 cm.
Cover title. Includes 5 papers, 1 verbal statement, 1 of the 2 addresses, statement of concern.
KF4770.A75 C65 1973

Conference on Computers: Privacy and Freedom of Information, Queen's University, 1970.
Conference on Computers: Privacy and Freedom of Information. [Ottawa, Information Canada, 1971]
108 p. 28 cm. (Telecommission study 5b)
$2.00
JC599.C2 C65 1970

Congressional Quarterly, inc.
Crime and justice in America. [Editor: Joseph Foote] 2d ed. Washington, 1968.
92 p. illus. 28 cm. (CQ background) 3.95
"A publication of Congressional Quarterly Service." Includes bibliographical references.
KF9223 .Z9C6 1968
345/.73/05
68-59304

Copeland, Miles.
Without cloak or dagger; the truth about the new espionage. New York, Simon and Schuster [1974]
351 p. 23 cm. $8.95
Includes bibliographical references.
UB270 .C66

Cortés, Irene R., 1921-
The constitutional foundations of privacy [by] Irene R. Cortes. [Quezon City, Division of Publications, U.P. Law Center, 1970]
105 p. 23 cm. (Albino Z. SyCip lecture series, 1970)
Bibliography: p. 83-89.
LAW

Council of Europe. Committee of Experts on the Protection of Privacy.
Protection of the privacy of individuals vis-a-vis electronic data banks in the private sector : resolution (73) 22 adopted by the Committee of Ministers of the Council of Europe on 26 September 1973 : and explanatory report / [prepared by the Committee of Experts on the Protection of Privacy]. Strasbourg : Council of Europe, 1974.
20 p. ; 24 cm.
LAW

Cowan, Paul.
State secrets; police surveillance in America [by] Paul Cowan, Nick Egleson, and Nat Hentoff, with Barbara Herbert and Robert Wall. [1st ed.] New York, Holt, Rinehart and Winston [1974]
xi, 333 p. 22 cm.
Includes bibliographical references.
JC599.U5 C67

Coven, Zelman.
The private man. Sydney, Australian Broadcasting Commission, 1969.
64 p. 18 cm. (The Boyer lectures, 1969)
$0.30
LAW

Cragan, John F.
Government surveillance of U.S. citizens: issues and answers [by] John F. Cragan [and] Donald C. Shields. Minneapolis, Campus Press [1971]
111 p. 23 cm.
Bibliography: p. 95-111.
KF1262 .Z8C7

Cray, Ed.
The enemy in the streets; police malpractice in America. Garden City, N.Y., Anchor Books, 1972.
345 p. 18 cm. $2.50
"An extensively revised, expanded, and updated version of The big blue line."
Includes bibliographical references.
KF9223 .C72

Cunningham, John Edward, 1923-
Security electronics, by John E. Cunningham. [1st ed.] Indianapolis, H. W. Sams [1970]
159 p. illus. 22 cm. 4.50
TH9739 .C85

Dash, Samuel.
The eavesdroppers [by] Samuel Dash, Richard F. Schwartz [and] Robert E. Knowlton. New York, Da Capo Press, 1971 [c1959]
484 p. illus. 24 cm. (Civil liberties in American history)
Bibliography: p. 379-381.
HV8073.5 .D3 1971
364.12
ISBN 0306700743

71-136488

Dial, O. Eugene.
Privacy, security, and computers : guidelines for municipal and other public information systems / O. E. Dial, Edward M. Goldberg. New York : Praeger, 1975.
ix, 169 p. ; 25 cm. (Praeger special studies in U.S. economic, social, and political issues)
Includes index. Bibliography: p. 150-165.
JS344.E4 D5 1975

Deacon, Richard.
A history of the British secret service. London, Muller, 1969.
440 p. 12 plates, illus., ports. 23 cm. 70/-
Bibliography: p. 430-431.
JN329.I6 D4 1969

Data Communications Symposium, 4th, Quebec, 1975.
Network structures in an evolving operational environment : fourth Data Communications Symposium, 7-9 October, 1975, Quebec City, Canada. New York : Institute of Electrical and Electronics Engineers, c1975.
174 p. in various pagings : ill. ; 28 cm.
Sponsored by Special Interest Group on Data Communications of the Association for Computing Machinery, Technical Committee on Computer Communications of the IEEE Computer Society, and Technical Committee on Data Communication Systems of the IEEE Communications Society. Includes bibliographical references.
TK5105.5 .D335 1975

Dulles, Allen Welsh, 1893-1969.
The craft of intelligence. [1st ed.] New York, Harper & Row [1963]
viii, 277 p. illus., ports. 22 cm.
Bibliography: p. 265-267.
UB270 .D8

Dunn, Edgar Streeter.
Social information processing and statistical systems--change and reform [by] Edgar S. Dunn, Jr. New York, Wiley [1974]
x, 246 p. illus. 23 cm.
"A Wiley-Interscience publication."
Bibliography: p. 234-240.
Z699.5.S65 D85 1974

Dvornik, Francis, 1893-
Origins of intelligence services: the ancient Near East, Persia, Greece, Rome, Byzantium, the Arab Muslim Empires, the Mongol Empire, China, Muscovy. New Brunswick, N.J., Rutgers University Press [1974]
xvi, 334 p. illus. 24 cm.
Includes bibliographies.
UB250 .D86 1974

Eldefonso, Edward, comp.
Readings in criminal justice. New York, Glencoe Press [1973]
xi, 530 p. 25 cm. (Glencoe Press criminal justice series)
Includes bibliographies.
HV7921 .E43

Ernst, Morris Leopold, 1888-
Privacy: the right to be let alone, by Morris L. Ernst and Alan U. Schwartz. London, MacGibbon & Kee, 1968.
ix, 238 p. 23 cm. 36/-
KF1262 .E7 1968
323.44
68-132013

Exploring privacy and data security costs : a summary of a workshop : a report of the NBS Workshop on Privacy and Data Security Costs, February 20, 1975, Gaithersburg, Maryland / edited by John L. Berg ; Gary D. Bearden, chairman ; [sponsored by] Systems and Software Division, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. Washington : U.S. Dept. of Commerce, National Bureau of Standards : for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1975.
vi, 28 p. ; 26 cm. (NBS technical note ; 876)
QC100 .U5753 no. 876 HF5548.2

Farago, Ladislas.
The game of the foxes : British and German intelligence operations and personalities which changed the course of the Second World War / by Ladislas Farago. London : Hodder and Stoughton, 1972.
xxi, 696 p. ; 25 cm.
Includes index. Bibliography: p. 661-679.
D810.S7 F33 1972b

Farago, Ladislas.
The game of the foxes; the untold story of German espionage in the United States and Great Britain during World War II. New York, D. McKay Co. [1972, c1971]
xxi, 696 p. 25 cm. $11.95
Bibliography: p. 661-679.
D810.S7 F33

Farago, Ladislas.
War of wits : the anatomy of espionage and intelligence / by Ladislas Farago. Westport, Conn. : Greenwood Press, 1976, c1954.
p. cm.
Reprint of the ed. published by Funk & Wagnalls, New York.
UB250 .F3 1976

Felkenes, George T., comp.
Police patrol operations: purpose, plans, programs, and technology; readings compiled and edited by George T. Felkenes and Paul M. Whisenand. Berkeley, Calif., McCutchan Pub. Corp. [1972]
vii, 339 p. illus. 23 cm.
Includes bibliographical references.
HV8080.P2 F45

Ferguson, Robert J.
The polygraph in court, by Robert J. Ferguson and Allan L. Miller. Springfield, Ill., Thomas [1973]
xxv, 346 p. illus. 24 cm. $14.95
Bibliography: p. 322.
KF9666 .F474

Ferguson, Robert J.
The scientific informer, by Robert J. Ferguson, Jr. Springfield, Ill., Thomas [1971]
xvii, 227 p. 24 cm.
Includes bibliographical references.
HV8078 .F43

Fitzgibbon, Constantine.
Secret intelligence in the twentieth century / Constantine Fitzgibbon. New York : Stein and Day, [1976]
p. cm.
UB250 .F57

Flaherty, David H.
Privacy in colonial New England [by] David H. Flaherty. Charlottesville, University Press of Virginia [1972]
xii, 287 p. 25 cm.
Bibliography: p. [253]-273.
JC599.U52 A113
323.44/0974
ISBN 0813903394
76-154804

Fraser, Gordon.
Modern transportation and international crime. With a foreword by Quinn Tamm. Springfield, Ill., Thomas [1970]
vii, 108 p. illus., ports. 24 cm.
HV8073 .F69

French, Scott R.
The big brother game / Scott R. French. San Francisco : Gnu Pub., c1975.
237 p. : ill. ; 28 cm.
JC597 .F73

Gellman, H. S.
Statistical data banks and their effects on privacy : a study for the Privacy and Computers Task Force / H. S. Gellman. [Ottawa] : Dept. of Communications, [1973?]
47 p. ; 28 cm.
JC599.C2 G45

Gibson, R. Dale.
Privacy and commercial reporting agencies by R. Dale Gibson and John M. Sharp. Winnipeg, Legal Research Institute of the University of Manitoba, 1968.
31 p. 23 cm. (Privacy and the law research report no. 1) unpriced
Bibliographical footnotes.
LAW

Godfrey, Edwin Drexel, 1921-
Basic elements of intelligence; a manual of theory, structure and procedures for use by law enforcement agencies against organized crime, by E. Drexel Godfrey, Jr. and Don R. Harris. Washington, Technical Assistance Division, Office of Criminal Justice Assistancé, Law Enforcement Assistance Administration, Dept. of Justice; for sale by the Supt. of Doc., U.S. Govt. Print. Off., 1971.
xiii, 150 p. illus. 26 cm. $1.25
Bibliography: p. 144-150.
HV8141 .G63

Goldstein, Robert C.
The cost of privacy : operational and financial implications of databank-privacy regulation / Robert C. Goldstein. [Brighton, Me.] : Honeywell Information Systems, c1975.
xii, 150 p. ; 22 cm.
Includes bibliographical references.
HD9696.C62 G64

Great Britain. Committee on Privacy.
Report. London, H.M. Stationery Off., 1972.
xi, 349 p. 25 cm. ([Great Britain. Parliament. Papers by command] cmnd. 5012.) £2.00
At head of title: Home Office, Lord Chancellor's Office, Scottish Office. Chairman: Kenneth Younger. Includes bibliographical references.
KD1956 .P7

Greenawalt, R. Kent, 1936-
Legal protections of privacy : final report to the Office of Telecommunications Policy, Executive Office of the President / by Kent Greenawalt. Washington : Office of Telecommunications Policy, Executive Office of the President, [1975]
xxi, 130 p. ; 26 cm.
KF1262 .G7

Harris, William Robert, 1941-
Intelligence and national security; a bibliography with selected annotations, by William R. Harris. [Cambridge? Mass., 1968]
3 v. (xcii, 838 l.) 30 cm.
Z6724.I7 H3

Harrison, Annette.
The problem of privacy in the computer age: an annotated bibliography. Santa Monica, Calif., Rand Corp., 1967-68 [c1970]
2 v. 28 cm. (Rand Corporation. Memorandum. RM-5495-PR/RC--RM-5495/1-PR/RC)
"Research ... supported by the United States Air Force under Project Rand--contract no. F44620-67-C-0045."
0180.A1 R36 no. 5495
016.32344

Haswell, Chetwynd John Drake, 1919-
British military intelligence [by] Jock Haswell. London, Weidenfeld and Nicolson, 1973.
xiii, 262, [8] p. illus., map, ports. 23 cm. £4.85
Bibliography: p. 251-253.
UB251.G7 H37

Hellman, J. J.
Privacy and information systems; an argument and an implementation [by] J. J. Hellman. [Santa Monica, Calif., Rand Corp.] 1970.
76 p. illus., form. 28 cm. ([Rand Corporation. Paper] P-4298)
Thesis (M.S.)--Massachusetts Institute of Technology. Bibliography: p. 76.
AS36 .R28 no. 4298 JC597

Henshaw, John R.
Computerised dossier compilation [by] John R. Henshaw. [Melbourne, Victorian Council for Civil Liberties] 1968.
4 p. 34 cm. unpriced
Cover title. At head of title: First Australian Convention, Councils for Civil Liberties, Sydney, 1968.
LAW

Hicks, Randolph D.
Undercover operations and persuasion [by] Randolph D. Hicks, II. Springfield, Ill., C. C. Thomas [1973]
xi, 91 p. 24 cm.
Bibliography: p. 81.
HV8080.U5 H5

Hoffman, Lance J., comp.
Security and privacy in computer systems. [Compiled by] Lance J. Hoffman. Los Angeles, Melville Pub. Co. [1973]
ix, 422 p. 23 cm. (Information sciences series)
HF5548.2 .H584

Hondius, Frederik Willem, 1927-
Emerging data protection in Europe / Frits W. Hondius. Amsterdam : North-Holland Pub. Co. ; New York : American Elsevier Pub. Co., 1975.
ix, 282 p. ; 23 cm.
Includes index. Bibliography: p. [271]-275.
LAW

How to avoid electronic eavesdropping and privacy invasion. Los Angeles, Investigator's Information Service [1967]
52 p. illus. 22 cm.
TK7882.E2 H6

Hunt, Madelyn Kathleen, 1948-
Privacy and security in databank systems : an annotated bibliography, 1970-1973 / M. Kathleen Hunt, Rein Turn. Santa Monica : Rand, 1974.
xiv, 166 p. ; 28 cm. ([Report] - Rand Corporation ; R-1361-NSF)
AS36 .R3 R-1361 Z7164.L6 JC597
081 s 016.32344

Illinois. Secure Automated Facility Environment Project.
The elements and economics of information privacy and security. [Springfield] : Secure Automated Facility Environment Project, [1974]
iii, 123, [68] p. : ill. ; 28 cm.
Cover title.
JC599.U5 I44 1974

International Colloquy about the European Convention on Human Rights, 3rd, Brussels, 1970.
Privacy and human rights; reports and communications presented at the third international colloquy about the European convention on human rights, organised by the Belgian Universities and the Council of Europe, with the support of the Belgian government, Brussels, 30 September - 3 October 1970. Edited by A. H. Robertson. Manchester, University Press [1973]
xiii, 457 p. 23 cm. £6.00
Distributed in the U.S.A. by Humanities Press, New York. Includes bibliographical references.
LAW

Irving, Clifford.
Spy: the story of modern espionage [by] Clifford Irving and Herbert Burkholz. [New York] Macmillan [1969]
206 p. illus., ports. 22 cm.
Bibliography: p. [200]-202.
UB270 .I69

Johnson, Timothy.
Teletext : data transmission by television / by Timothy Johnson. London : Financial Times, [1975]
[10], 187 p. : ill. ; 30 cm.
Includes bibliographical references.
TK6643 .J64

Jones, Mervyn, comp.
Privacy, compiled and edited by Mervyn Jones. Newton Abbot [Eng.] North Pomfret, Vt., David & Charles [1974]
230 p. 23 cm. (David & Charles sources for contemporary issues series) £5.25
Bibliography: 221-222.
JC599.G7 J65

Jones, Raymond Nelson, 1928-
Electronic eavesdropping techniques and equipment : prepared for the National Institute of Law Enforcement and Criminal Justice, Law Enforcement Assistance Administration, U.S. Department of Justice / by Raymond N. Jones. Washington : The Institute : for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1975 [i.e. 1976]
p. cm.
At head of title: Law enforcement standards program. "LESP-RPT-0207.00." Bibliography: p.
HV8073.5 .J65 1976

Justice Society. Committee on Privacy.
Privacy and the law: a report by Justice; Joint chairmen of Committee Mark Littman, Peter Carter-Ruck. London, Stevens, 1970.
[5], 65 p. 25 cm. 16/-
Includes bibliographical references.
LAW

Kent, Graeme.
Espionage / [by] Graeme Kent. London : Batsford, 1974.
96 p. : ill., facsims., ports. ; 22 cm.
(Past-into-present series)
Includes bibliographies and index.
UB270.5 .K46

Kirkpatrick, Lyman B.
The U.S. intelligence community: foreign policy and domestic activities [by] Lyman B. Kirkpatrick, Jr. New York, Hill and Wang [1973]
xi, 212 p. illus. 21 cm. $7.95
Includes bibliographical references.
JK468.I6 K53 1973

Lamoreux, Stephen.
The right of privacy; a bibliography: 71 years, 1890-1961 [by] Stephen Lamoreux. [Pullman? 1962?]
x, 60 p. 28 cm.
Cover title.
KF1262 .A1L3

Lapidus, Edith J.
Eavesdropping on trial [by] Edith J. Lapidus. Rochelle Park, N.J., Hayden Book Co. [1973, c1974]
287 p. 24 cm. $7.95
Bibliography: p. 242-247.
KF9670 .L37

Laver, Murray.
Computers, communications and society / Murray Laver. London ; New York : Oxford University Press, 1975.
99 p. : ill. ; 22 cm. (Science and engineering policy series)
Includes index. Bibliography: p. 94.
TK5105.5 .L38

Law Enforcement Effectiveness Conference, Washington, D.C., 1974.
Law Enforcement Effectiveness Conference. Washington : National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, 1976.
p. cm. (Supporting materials for the Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance)
KF9670.A75 L3 1974

Lee, Peter G.
Interpol / by Peter G. Lee. New York : Stein and Day, [1976]
p. cm.
HV7240 .L43

Legal admissibility of the polygraph, compiled and edited by Norman Ansley. Springfield, Ill., Thomas [1974, c1975]
xiii, 344 p. illus. 27 cm.
Papers presented at a symposium held at the 7th annual seminar of the American Polygraph Association in Chicago, 1972. Bibliography: p. 328-337.
KF9666.A75 L4

LeMond, Alan.
No place to hide / by Alan LeMond and Ron Fry. New York : St. Martin's Press, [1975]
xxvi, 278 p. : ill. ; 22 cm. (A New earth book)
Includes index. Bibliography: p. 265-267.
JC599.U5 L42

Liston, Robert A.
The dangerous world of spies and spying [by] Robert Liston. New York, Platt & Munk [1967]
274 p. 23 cm.
Bibliography: p. [273]-274.
UB270 .L5

Long, Edward V., 1908-
The intruders; the invasion of privacy by government and industry, by Edward V. Long. With a foreword by Hubert H. Humphrey. New York, Praeger [1967, c1966]
viii, 230 p. illus. 22 cm.
JC599.U5 L6

Lowi, Theodore J., comp.
Private life and public order; the context of modern public policy, edited with an introd. by Theodore J. Lowi. [1st ed.] New York, Norton [1968]
xxi, 198 p. 21 cm. (Problems of modern government)
Bibliography: p. 197-198.
HD3616.U46 L6

Madgwick, Donald.
The invasion of privacy [by] Donald Madgwick and Tony Smythe. [London, New York] Pitman [1974]
ix, 197 p. 23 cm. £3.50
Bibliography: p. 191-192.
JC599.G7 M33

Manning, Morris.
The protection of privacy act, bill C-176 : an analysis and commentary / Morris Manning. Toronto : Butterworths, [c1974]
xxii, 200 p. ; 23 cm. (Canadian annotated legislation series)
Includes index.
LAW

Martin, James, 1933-
Security, accuracy, and privacy in computer systems. Englewood Cliffs, N.J., Prentice-Hall [1973]
xiv, 626 p. illus. 24 cm. (Prentice-Hall series in automatic computation)
Includes bibliographical references.
HF5548.2 .M342

Massachusetts. Governor's Commission on Privacy and Personal Data.
Privacy and student records : a report with recommendations and guidelines. [Boston] : Governor's Commission on Privacy and Personal Data, 1974.
42 leaves ; 28 cm.
Cover title.
KFM2792 .A824

Massachusetts. Governor's Commission on Privacy and Personal Data.
Report of the director / Governor's Commission on Privacy and Personal Data. [Boston] : The Commission, 1974.
31 leaves ; 28 cm.
Cover title.
JC599.U52 M29 1974

Mayer, Michael F.
Rights of privacy, by Michael F. Mayer. New York, Law-Arts Publishers, 1972.
xvi, 253 p. 24 cm. $7.95
Bibliography: p. 252-253.
KF1262 .M39

McChristian, Joseph A.
The role of military intelligence, 1965-1967 / by Joseph A. McChristian. Washington : Dept. of the Army : for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1974 [i.e. 1975]
x, 182 p. : ill. ; 24 cm. (Vietnam studies)
Title on spine: Military intelligence.
Includes index.
DS558.9 .M54M3

Miller, Arthur Raphael, 1934-
The assault on privacy: computers, data banks, and dossiers [by] Arthur R. Miller. Ann Arbor, University of Michigan Press [1971]
xiv, 333 p. 24 cm. $7.95
Bibliography: p. 261-269.
JC599.U5 M49

National Academy of Sciences, Washington, D.C. Project on Computer Databanks.
Databanks in a free society; computers, record-keeping, and privacy: report [by] Alan F. Westin, project director [and] Michael A. Baker, assistant project director. [New York] Quadrangle Books [1972]
xxi, 522 p. 25 cm. $12.50
Includes bibliographical references.
JC599.U5 N28 1972

National Research Council. Committee on Federal Agency Evaluation Research.
Protecting individual privacy in evaluation research / The Committee on Federal Agency Evaluation Research, Assembly of Behavioral and Social Sciences, National Research Council. Washington : National Academy of Sciences, 1975.
15, A25, B86 p. ; 28 cm.
"Confidentiality-preserving modes of access to files and to interfile exchange for useful statistical analysis" by D. T. Campbell, et al.: p. A1-A25. "A researcher's shield statute" by P. Nejelski and H. Peyser: p. B1-B86. Bibliography: p. A22-A25.
JC599.U5 N35 1975

Neier, Aryeh, 1937-
Dossier : the secret files they keep on you / Aryeh Neier. New York : Stein and Day, 1975, c1974.
216 p. : 25 cm.
Includes bibliographical references and index.
JC599.U5 N44 1975

New York (State). Legislature. Joint Committee on Investigations of Public Service Commissions.
Wiretapping in New York City. New York, Arno Press, 1974.
1 v. (various pagings) 23 cm. (Criminal Justice in America)
Excerpts reprinted from v. 5 of Minutes and testimony of the Joint Legislative Committee Appointed to Investigate the Public Service Commissions, originally published in 1916 by J. B. Lyons Co., Albany.
KFN6168 .A2 1916b

New York (State). State Identification and Intelligence System.
A new concept in criminal justice information-sharing: NYSIIS, the New York State Identification and Intelligence System; system development plan. [Albany, 1966]
xii, 131 p. illus. (2 fold.; part col.) 28 cm.
Pref. signed: Robert R. J. Gallati, director.
HV7282 .A6 1966

Niblett, G. B. F.
Digital information and the privacy problem [by] G. B. F. Niblett. [Paris] Organisation for Economic Co-operation and Development [1971]
58 p. 24 cm. (OECD informatics studies, 2) $2.00 (U.S.)
Includes bibliographical references.
JC597 .N5

On record : files and dossiers in American life / edited by Stanton Wheeler. New Brunswick, N.J. : Transaction Books, c1976.
p. cm. (Law and society ; 1)
Includes index.
JC599.U5 O48 1976

Packard, Vance Oakley, 1914-
The naked society [by] Vance Packard.
Harmondsworth, Penguin, 1966.
322 p. 18 1/2 cm.
"Reference notes" p. 301-305.
JC599.U5 P36 1966

Pember, Don R., 1939-
Privacy and the press: the law, the mass media, and the First amendment, by Don R. Pember. Seattle, University of Washington Press [1972]
xiii, 298 p. 24 cm. $8.95
Bibliography: p. 287-291.
KF1262 .P4

Pollock, David A.
Methods of electronic audio surveillance, by David A. Pollock. Springfield, Ill., Thomas [1973]
xvii, 385 p. illus. 24 cm.
Bibliography: p. 375-379.
TK7882.E2 P64

Privacy. Edited by J. Roland Pennock and John W. Chapman. [1st ed.] New York, Atherton Press, 1971.
xx, 255 p. 22 cm. (Nomos, 13)
Includes bibliographical references.
JC599.U5 P75

Privacy / [chairman, Stanley S. Arkin]. New York : Practising Law Institute, [1974]
440 p. ; 22 cm. (Criminal law and practice course handbook series ; no. 70)
"C4-3187." "Prepared for distribution at the Privacy Program, August-September 1974." Pages 436-440 blank. Bibliography: p. 373-405.
KF1262.Z9 P7

Privacy : a summary of a Seminar on Privacy, December 15-17, 1974, Washington, D.C. / the Domestic Council Committee on the Right of Privacy and the Council of State Governments, in cooperation with the National Governors' Conference ... [et al.]. Lexington, Ky. : Council of State Governments, 1975.
vii, 64 p. ; 23 cm.
KF1262.A75 P74

Private rights and freedom of the individual: report of a conference at Ditchley Park, 7-10 April 1972, by C. F. O. Clarke. Enstone, Ditchley Foundation, [1972].
39 p. 23 cm. (Ditchley paper, no. 41)
£0.40
JC597 .P74

Project Search. Committee on Security and Privacy.
Security and privacy considerations in criminal history information systems. Robert Gallati, chairman. [Sacramento] 1970.
v, 56 p. 23 cm. ([Project Search.] Technical report no. 2)
Cover title.
Z699.5.C7 P76

Raines, John C.
Attack on privacy [by] John Curtis Raines. Valley Forge [Pa.] Judson Press [1974]
144 p. 22 cm.
Includes bibliographical references.
JC599.U5 R24

Ransom, Harry Howe, 1922-
The intelligence establishment. [Rev. and enl.] Cambridge, Mass., Harvard University Press, 1970.
xvi, 309 p. illus. 25 cm. 9.95
First ed. published in 1958 under title: Central intelligence and national security.
Bibliography: p. 274-285.
JK468.I6 R3 1970

Reed, Irving S.
The application of information theory to privacy in data banks [by] Irving S. Reed. Santa Monica, Rand, 1973.
ix, 60 p. illus. 28 cm. (Rand Corporation. [Rand report] R-1282-NSF)
"Prepared for the National Science Foundation." Includes bibliographical references.
AS36 .R3 R-1282 HF5548.2

Reed, Irving S.
Information theory and privacy in data banks [by] I. S. Reed. [Santa Monica, Calif., Rand Corp.] 1973.
iii, 24 p. 28 cm. (Rand Corporation. [Paper] P-4952)
Cover title. Bibliography: p. 24.
AS36 .R28 no. 4952 HF5548.2

Reid, John E.
Truth and deception : the polygraph (lie-detector) technique / John E. Reid, Fred E. Inbau. 2d ed. Baltimore : Williams & Wilkins Co., c1976.
p. cm.
Includes bibliographical references and index.
HV8078 .R4 1976

Renninger, Clark R.
Government looks at privacy and security in computer systems; a summary of a conference held at the National Bureau of Standards, Gaithersburg, Maryland, November 19-20, 1973. Clark R. Renninger and Dennis K. Branstad, editors. [Washington] National Bureau of Standards; [for sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1974.
vii, 37 p. 27 cm. (NBS Technical note 809) $0.85
Includes bibliographical references.
QC100 .U5753 no. 809 JC599.U5

The Right of privacy; a symposium on the implications of Griswold v. Connecticut, 381 U.S. 497 (1965) [by] Robert G. Dixon, Jr. [and others] New York, Da Capo Press, 1971 [c1965]
147 p. 24 cm. (Symposia on law and society)
Originally published in the Michigan law review, v. 64, no. 2 (Dec. 1965) under title: Symposium on the Griswold case and the right of privacy. Includes bibliographical references. CONTENTS: The Griswold penumbra: constitutional charter for an expanded law of privacy? By R. G. Dixon, Jr. Nine justices in search of a doctrine, by T. I. Emerson. Penumbras, peripheries, emanations, things fundamental and things forgotten: the Griswold case, by P. G. Kauper. The right of privacy: emanations and intimations, by R. B. McKay. Privacy in Connecticut, by A. E. Sutherland. Supplement: Griswold v. Connecticut (381 U.S. 479, 1965)
KF1262 .A75R5

The Right to privacy / edited by Grant S. McClellan. New York : H. W. Wilson Co., 1976.
240 p. ; 20 cm. (The Reference shelf ; v. 48, no. 1)
Bibliography: p. 233-240.
KF1262.A75 R52

Rosenberg, Jerry Martin.
The death of privacy [by] Jerry M. Rosenberg. New York, Random House [1969]
xvi, 236 p. 22 cm. 6.95
Includes bibliographical references.
JC599.U5 R64

Rowan, Richard Wilmer, 1894-
Secret service: thirty-three centuries of espionage, by Richard Wilmer Rowan with Robert G. Deindorfer. London, Kimber, 1969.
xiii, 786 p. facsims. 23 cm. 70/-
Revised ed. of The story of secret service by Richard Wilmer Rowan, New York, Doubleday, Doran, 1937.
UB270 .R57 1969

Rule, James B., 1943-
Private lives and public surveillance [by] James B. Rule. [London] Allen Lane [1973]
382 p. 23 cm. £3.50
JC599.G7 R84

Rule, James B., 1943-
Private lives and public surveillance; social control in the computer age [by] James B. Rule. New York, Schocken Books [1974]
382 p. 22 cm.
Includes bibliographical references.
JC599.G7 R84 1974

Search Group.
Standards for security and privacy of criminal justice information / submitted by SEARCH Group, Inc. Sacramento, Calif. : The Group, 1975.
iii, 20 p. ; 28 cm. (Technical report - SEARCH Group ; no. 13)
Includes bibliographical references.
Z699.5.C7 S4 1975

Seth, Ronald.
Encyclopedia of espionage. Garden City, N.Y., Doubleday [1974, c1972]
718 p. 22 cm. $10.00
UB270 .S4385 1974

Severn, William.
The right to privacy, by Bill Severn. [New York] I. Washburn [1973]
186 p. 21 cm. $4.50
Bibliography: p. 177-179.
JC599.U5 S45

Sharp, John M.
Credit reporting and privacy; the law in Canada and the U.S.A. [by] John M. Sharp. Toronto, Butterworths [1970]
xv, 124 p. 23 cm. $6.95
Includes bibliographical references.
LAW

Shils, Edward Albert, 1911-
The torment of secrecy; the background and consequences of American security policies [by] Edward A. Shils. Carbondale, Southern Illinois University Press [1974, c1956]
238 p. 20 cm. (Arcturus books, AB127)
Reprint of the ed. published by Free Press, New York.
E743.5 .S48 1974

Slough, M. C.
Privacy, freedom, and responsibility, by M. C. Slough. Springfield, Ill., Thomas [c1969]
xviii, 323 p. 24 cm. (American lecture series, publication 753. A monograph in the Bannerstone division of American lectures in behavioral science law)
Includes bibliographical references.
KF8625 .S55

Snyder, Gerald S.
The right to be let alone : privacy in the United States / by Gerald S. Snyder. New York : J. Messner, [1975]
190 p. : ill. ; 21 cm.
Explores today's technological assault on privacy and some of the ways citizens can be protected from it. Includes index.
Bibliography: p. 183-184.
JC599.U5 S59

South Australia. Law Reform Committee.
Interim report of the Law Reform Committee of South Australia to the Attorney-General regarding the law of privacy. [Adelaide] [Govt. Pr.], 1973.
[17] p. 24 cm. $0.25
LAW

Spindel, Bernard B.
The ominous ear [by] Bernard B. Spindel. [1st ed.] New York, Award House [1968]
268 p. illus., ports. 21 cm.
JC599.US S64

St. George Jaycees.
Invasion of personal privacy; a report prepared by the St. George Jaycees. [Sydney, 1968]
40 p. 32 cm. 0.80
Presented by St. George Jaycees to 22nd National Convention, 1968. Bibliography: p. 40.
LAW

Steele, Alexander.
How to spy on the U.S. New Rochelle, N.Y., Arlington House [1974]
185 p. 24 cm.
E743.5 .S75

Sterling, James W.
Protecting dissent, policing disorder; an evaluation and documentation of the national political convention law enforcement service project. Prepared for the city of Miami Beach, Fla., by James W. Sterling, Ronald J. Bostick [and] Donald C. Dilworth. Gaithersburg, Md., Professional Standards Division, International Association of Chiefs of Police [1974]
x, 485 p. illus. 26 cm.
HV8148.M45 S73

Strömholm, Stig.
Right of privacy and rights of the personality. A comparative survey. (Working paper prepared for the Nordic Conference on Privacy organized by the International Commission of Jurists, Stockholm, May 1967.) Stockholm, Norstedt, 1967.
250 p. 22 cm. (Acta Instituti Upsaliensis Iurisprudentiae Comparativae, 8) 25.- skr
Bibliography: p. 245-247.
LAW

Strong, Kenneth, Sir, 1900-
Intelligence at the top: the recollections of an intelligence officer. London, Cassell, 1968.
271 p. 8 plates, illus., 3 facsims., 2 maps, ports. 22 cm. 42/-
"A Giniger book." Bibliography: p. 250.
D810.S7 S87

Strong, Kenneth, Sir, 1900-
Men of intelligence: a study of the roles and decisions of chiefs of intelligence from World War I to the present day. London, Cassell, 1970.
[14], 183 p., 8 plates. illus., ports. 22 cm. 50/-
"A Giniger book." Bibliography: p. 171-173.
UB250 .S66

Strong, Kenneth, Sir, 1900-
Men of intelligence; a study of the roles and decisions of chiefs of intelligence from World War I to the present day. [New York] St. Martin's Press [1972, c1971]
183 p. illus. 23 cm.
"A Giniger book." Bibliography: p. 171-173.
UB250 .S66 1972

Surveillance and espionage in a free society; a report by the planning group on intelligence and security to the Policy Council of the Democratic National Committee. Edited by Richard H. Blum. Foreword by Adlai E. Stevenson III. New York, Praeger Publishers [1972]
xxxii, 319 p. 25 cm. (Praeger special studies in international politics and government) $17.50
Includes bibliographical references.
JK468.I6 S95

Surveillance, dataveillance, and personal freedoms; use and abuse of information technology; a symposium edited by the staff of Columbia human rights law review. Foreword by Nat Hentoff. [Rev. and augm. text] Fair Lawn, N.J., R. E. Burdick, [1973]
247 p. 24 cm. $9.00
"Original text published as pages 1-235 of the Columbia human rights law review, volume 4, number 1." Includes bibliographical references.
JC597 .S95 1973

Task Force on Privacy and Computers.
Privacy and computers; a report of a Task Force established jointly by Dept. of Communications/Dept. of Justice. [Ottawa, Information Canada, 1972]
236 p. illus. 24 cm. $2.50
Includes bibliographical references.
JC599.C2 T37

Tregenza, Michael.
Espionage / [by] Michael Tregenza. London ; New York [etc.] : Hamlyn, 1974.
127 p. : col. ill., col. ports. ; 18 cm. (Hamlyn all-colour paperbacks)
Includes index. Bibliography: p. [124]
JF1525.I6 T73

Turn, R.
A brief history of computer privacy/security research at Rand [by] R. Turn [Santa Monica, Calif., Rand Corp.] 1972.
8 p. 28 cm. ([Rand Corporation. Paper] P-4798)
Cover title. Includes bibliographical references.
AS36 .R28 no. 4798 JC599.U5

Turn, R.
Privacy and security in databank systems: measures of effectiveness, costs, and protector-intruder interactions [by] Rein Turn and Norman Z. Shapiro. [Santa Monica, Rand Corp.] 1972.
36 p. illus. 28 cm. ([Rand Corporation, Paper] P-4871)
Cover title. Research supported by the National Science Foundation grant no. GI-29843. Bibliography: p. 35-36.
AS36 .R28 no. 4871 JC599.U5

Turn, R.
Privacy and security in personal information databank systems : prepared for the National Science Foundation. / Rein Turn. Santa Monica, Ca. : Rand, 1974.
xvii, 104 p. : ill. ; 28 cm. ([Report] - Rand Corporation ; R-1044-NSF)
Bibliography: p. 97-104.
AS36 .R3 R-1044 JC597

Turn, R.
Privacy transformations for databank systems [by] Rein Turn. [Santa Monica, Calif., Rand Corp.] 1973.
iii, 47 p. 28 cm. (Rand Corporation. [Paper] P-4955)
Cover title. Includes bibliographical references.
AS36 .R28 no. 4955 HF5548.2

Turner, William W.
How to avoid electronic eavesdropping and privacy invasion, by William W. Turner. [Rev. ed. Los Angeles] Investigators Information Service [1972]
192 p. illus. 20 cm.
TK7882.E2 T87 1972

United States. Congress. House. Committee on Government Operations.
Unmet training needs of the Federal investigator and the consolidated Federal Law Enforcement Training Center; thirtieth report by the Committee on Government Operations. Washington, U.S. Govt. Print. Off., 1970.
v, 126 p. maps. 24 cm. (91st Congress, 2d session. House report no. 91-1429)
Based on a study made by the Legal and Monetary Affairs Subcommittee.
KF32.G6 1970d

United States. Congress. House. Committee on Government Operations.
The use of polygraphs and similar devices by Federal agencies : thirteenth report / by the Committee on Government Operations, together with separate and dissenting views. Washington : U.S. Govt. Print. Off., 1976.
vi, 61 p. ; 24 cm. (House report - 94th Congress, 2d session ; no. 94-795)
Includes bibliographical references.
JK468.L5 U553 1976

United States. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Access to records : hearings before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-third Congress, second session, on H.R. 12206 and related bills ... Washington : U.S. Govt. Print. Off., 1974.
iv, 338 p. ; 23 cm.
KF27 .G6594 1974

United States. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Availability of information from Federal departments and agencies (telephone monitoring--third review). Washington, U.S. Govt. Print. Off., 1970.
x, 52 p. 24 cm.
At head of title: Committee print. 91st Congress, 2d session. House of Representatives.
JC599.U5 A23

United States. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Executive orders 11697 and 11709 permitting inspection by the Department of Agriculture of farmers' income tax returns. Hearings before a subcommittee of the Committee on Government Operations, House of Representatives, Ninety-third Congress, first session. May 9 and August 3, 1973. Washington, U.S. Govt. Print. Off., 1973.
iii, 167 p. 24 cm.
KF27 .G6594 1973f

United States. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Federal information systems and plans--Federal use and development of advanced information technology. Hearings before a subcommittee of the Committee on Government Operations, House of Representatives, Ninety-third Congress, first session ... Washington, U.S. Govt. Print. Off., 1973-
v. illus. 24 cm. $1.85 (v. 1)
Hearings held Apr. 10- Includes bibliographical references.
KF27 .G6594 1973b

United States. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Telephone monitoring practices by Federal agencies : hearings before a subcommittee of the Committee on Government Operations, House of Representatives, Ninety-third Congress, second session, June 11 and 13, 1974. Washington : U.S. Govt. Print. Off., 1974.
iv, 293 p. : ill. ; 24 cm.
KF27 .G6594 1974c

United States. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
The use of polygraphs and similar devices by Federal agencies : hearings before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-third Congress, second session, June 4 and 5, 1974. Washington : U.S. Govt. Print. Off., 1974.
iv, 790 p. : ill. ; 24 cm.
KF27 .G6594 1974b

United States. Congress. House. Committee on Government Operations. Legal and Monetary Affairs Subcommittee.
Federal training programs for investigative personnel. Hearings before a subcommittee of the Committee on Government Operations, House of Representatives, Ninety-first Congress, second session. May 14, 20, and June 18, 1970. Washington, U.S. Govt. Print. Off., 1970.
v, 464 p. illus., forms, maps. 24 cm.
KF27.G667 1970

United States. Congress. House. Committee on Government Operations. Legislation and National Security Subcommittee.
Access of service secretaries to military information : hearing before a subcommittee of the Committee on Government Operations, House of Representatives, Ninety-fourth Congress, first session, September 10, 1975. Washington : U.S. Govt. Print. Off., 1975.
iii, 40 p. ; 24 cm.
KF27 .G6676 1975f

United States. Congress. House. Committee on Government Operations. Special Studies Subcommittee.
Federal involvement in the use of behavior modification drugs on grammar school children of the right to privacy inquiry. Hearing before a subcommittee of the Committee on Government Operations, House of Representatives, Ninety-first Congress, second session. September 29, 1970. Washington, U.S. Govt. Print. Off., 1970.
iii, 175 p. 24 cm. $0.65
KF27.G676 1970d

United States. Congress. House. Committee on Government Operations. Special Subcommittee on Invasion of Privacy.
The computer and invasion of privacy. Hearings, Eighty-ninth Congress, second session. July 26, 27, and 28, 1966. Washington, U.S. Govt. Print. Off., 1966.
iv, 318 p. 24 cm.
KF27 .GG665 1966a

United States. Congress. House. Committee on Government Operations. Special Subcommittee on Invasion of Privacy.
The computer and invasion of privacy. New York, Arno Press, 1967.
iv, 311 p. 24 cm.
Includes original t.p.: The computer and invasion of privacy; hearings before a subcommittee of the Committee on Government Operations, House of Representatives, Eighty-ninth Congress, second session, July 26, 27, and 28, 1966. Washington, U.S. Govt. Prin . Off., 1966.
KF27 .G665 1966b

United States. Congress. House. Committee on Government Operations. Subcommittee on Government Information and Individual Rights.
Implementation of the Privacy act of 1974 : data banks : hearing before a subcommittee of the Committee on Government Operations, House of Representatives, Ninety-fourth Congress, first session, June 3, 1975. Washington : U.S. Govt. Print. Off., 1975.
iii, 156 p. ; 24 cm.
KF27 .G6628 1975c

United States. Congress. House. Committee on Internal Security.
Domestic intelligence operations for internal security purposes : hearings before the Committee on Internal Security, House of Representatives, Ninety-third Congress, second session. Washington : U.S. Govt. Print. Off., 1974-
v. ; 23 cm.
Hearings held Feb. 20- 1974. Includes bibliographical references and index.
KF27 .I548 1974a

United States. Congress. House. Committee on Interstate and Foreign Commerce. Special Subcommittee on Investigations.
FCC monitoring of employees' telephones. Hearing, Ninety-second Congress, second session. March 28 and May 16, 1972. Washington, U.S. Govt. Print. Off., 1972.
iii, 82 p. 24 cm.
"Serial no. 92-101."
KF27 .I5545 1972b

United States. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Employee Benefits.
Invasion of Federal employees' privacy. Hearings, Ninety-second Congress, first session, on H.R. 7199 and related bills ... Washington, U.S. Govt. Print. Off., 1971.
iv, 432 p. 24 cm.
"Serial no. 92-17." Hearings held May 11-June 2, 1971.
KF27.P644 1971b

United States. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Manpower and Civil Service.
Privacy and the rights of Federal employees. Hearings, Ninetieth Congress, second session, on S. 1035 ... [and] H.R. 17760 ... Washington, U.S. Govt. Print. Off., 1968.
v, 436 p. forms. 23 cm.
Hearings held June 13-July 17, 1968.
"Serial no. 90-49."
KF27.P653 1968c

United States. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Postal Operations.
Privacy in the mail. Hearings, Ninetieth Congress, second session. July 23 and 24, 1968. Washington, U.S. Govt. Print. Off., 1968.
iii, 33 p. 24 cm.
"Serial no. 90-42."
HE6331 1968 .A516

United States. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Retirement and Employee Benefits.
Right to privacy of Federal employees : hearings before the Subcommittee on Retirement and Employee Benefits of the Committee on Post Office and Civil Service, House of Representatives, Ninety-third Congress, first and second sessions, on H.R. 1281 and related bills .... Washington : U.S. Govt. Print. Off., 1974.
iv, 378 p. ; 24 cm.
Hearings held May 14-Aug. 8, 1974. "Serial no. 93-22." Includes bibliographical references.
KF27 .P673 1974f

United States. Congress. House. Committee on the Judiciary. Subcommittee on Civil Rights and Constitutional Rights.
Dissemination of criminal justice information : hearings before the Subcommittee on Civil Rights and Constitutional Rights of the Committee on the Judiciary, House of Representatives, Ninety-third Congress, second session .... Washington : U.S. Govt. Print. Off., 1974.
v, 586 p. ; 24 cm.
Hearings held July 26, 1973-Apr. 3, 1974, on H.R. 188, 9783, 12574, and 12575. "Serial no. 44." Includes bibliographical references.
KF27 .J847 1973e

United States. Congress. House. Committee on the Judiciary. Subcommittee on Courts, Civil Liberties, and the Administration of Justice.
Surveillance : hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary, House of Representatives, Ninety-fourth Congress, first session .... Washington : U.S. Govt. Print. Off., 1975-
v. ; 24 cm.
"Serial no. 26." Hearings held Feb. 6-Sept. 8, 1975.
KF27 .J857 1975f

United States. Congress. House. Committee on the Judiciary. Subcommittee on Courts, Civil Liberties, and the Administration of Justice.
Wiretapping and electronic surveillance : hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary, House of Representatives, Ninety-third Congress, second session ... April 24, 26, and 29, 1974. Washington : U.S. Govt. Print. Off., 1974.
iv, 275 p. ; 24 cm.
Hearings on H.R. 1597, H.R. 7773, H.R. 9781, H.R. 9815, H.R. 9973, H.R. 10008, H.R. 10331, H.R. 11629, H.R. 11836, and H.R. 13825. "Serial no. 41."
KF27 .J857 1974h

United States. Congress. House. Committee on Un-American Activities.
Conduct of espionage within the United States by agents of foreign Communist governments. Hearings, Ninetieth Congress, first session. Washington, U.S. Govt. Print. Off., 1967.
iv, 553-713, iv p. illus. 24 cm.
Hearings held Apr. 6-Nov. 15, 1967.
UH271.R9 U5 1967

United States. Congress. House. Committee on Ways and Means.
Confidentiality of tax return information : hearing before the Committee on Ways and Means, House of Representatives, Ninety-fourth Congress, second session, January 28, 1976. Washington : U.S. Govt. Print. Off., 1976.
iv, 235 p. : ill. ; 24 cm.
KF27 .W3 1976a

United States. Congress. House. Committee on Ways and Means. Subcommittee on Oversight.
Internal Revenue Service intelligence operations : hearings before the Subcommittee on Oversight of the Committee on Ways and Means, House of Representatives, Ninety-fourth Congress, first session, March 26 and June 25, 1975. Washington : U.S. Govt. Print. Off., 1975.
iii, 100 p. ; 23 cm.
KF27 .W345 1975d

United States. Congress. House. Select Committee on Intelligence.
U.S. intelligence agencies and activities : intelligence costs and fiscal procedures : hearings before the Select Committee on Intelligence, U.S. House of Representatives, Ninety-fourth Congress, first session .... Washington : U.S. Govt. Print. Off., 1975-
v. : ill. ; 24 cm.
Hearings held July 31-Aug. 8, 1975.
KF27.5 .I5 1975

United States. Congress. Joint Economic Committee. Subcommittee on Economic Statistics.
Review of Federal statistical programs. Hearings, Ninety-first Congress, first session. April 30, May 1, and 15, 1969. Washington, U.S. Govt. Print. Off., 1969.
v, 208 p. 24 cm. 1.00
HA37 .U535

United States. Congress. Senate. Committee on Banking, Housing and Urban Affairs. Subcommittee on Financial Institutions.
The effect of the Bank secrecy act on State laws : hearings before the Subcommittee on Financial Institutions of the Committee on Banking, Housing and Urban Affairs, United States Senate, Ninety-third Congress, second session, on S. 2200 ... Los Angeles, Calif., July 26, 1974, San Francisco, Calif., July 29, 1974. Washington : U.S. Govt. Print. Off., 1974.
iii, 213 p. ; 24 cm.
Includes bibliographical references.
KF26 .B3943 1974e

United States. Congress. Senate. Committee on Finance. Subcommittee on Administration of the Internal Revenue Code.
Federal tax return privacy : hearings before the Subcommittee on Administration of the Internal Revenue Code of the Committee on Finance, United States Senate, Ninety-fourth Congress, first session. Washington : U.S. Govt. Print. Off., 1975.
iv, 308 p. : ill. ; 24 cm.
KF26 .F55385 1975

United States. Congress. Senate. Committee on Foreign Relations.
Dr. Kissinger's role in wiretapping : hearings before the Committee on Foreign Relations, United States Senate, Ninety-third Congress, second session.... Washington : U.S. Govt. Print. Off., 1974.
x, 409 p. ; 24 cm.
Executive hearings held Jan. 29-Sept. 29, 1974.
KF26 .F6 1974k

United States. Congress. Senate. Committee on Foreign Relations.
Intelligence and the ABM. Hearing, Ninety-first Congress, first session ... June 23, 1969. Washington, U.S. Govt. Print. Off., 1969.
xi, 76 p. 23 cm.
UG633 .A413 1969

United States. Congress. Senate. Committee on Foreign Relations.
Report on the inquiry concerning Dr. Kissinger's role in wiretapping, 1969-1971 : review and findings / by the Committee on Foreign Relations, United States Senate.
Washington : U.S. Govt. Print. Off., 1974.
ii, 6 p. ; 23 cm.
At head of title: 93d Congress, 2d session. Committee print.
JC599.U5 U53 1974d

United States. Congress. Senate. Committee on Foreign Relations. Subcommittee on Surveillance.
Warrantless wiretapping and electronic surveillance : report / by the Subcommittee on Surveillance of the Committee on Foreign Relations, United States Senate, and the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary, United States Senate. Washington : U.S. Govt. Print. Off., 1975.
iii, 11 p. ; 24 cm.
At head of title: 94th Congress, 1st session. Committee print.
KF9670 .A25 1975

United States. Congress. Senate. Committee on Government Operations.
Materials pertaining to S. 3418 and protecting individual privacy in Federal gathering, use, and disclosure of information / compiled by staff of the Committee on Government Operations, United States Senate.
Washington : U.S. Govt. Print. Off., 1974.
v, 103 p. ; 24 cm.
At head of title: 93d Congress, 2d session. Committee print. Includes bibliographical references.
KF5752 .A25 1974

United States. Congress. Senate. Committee on Government Operations.
Privacy and protection of personal information in Europe : privacy developments in Europe and their implications for United States policy : a staff report of the Committee on Government Operations, United States Senate. Washington : U.S. Govt. Print. Off., 1975.
vii, 436 p. ; 24 cm.
At head of title: 93d Congress, 2d session. Committee print.
LAV

United States. Congress. Senate. Committee on Government Operations.
Senate Committee on Intelligence Activities : report of the Committee on Government Operations, United States Senate, to accompany S. Res. 400, resolution to establish a standing committee of the Senate on intelligence activities, and for other purposes. Washington : U.S. Govt. Print. Off., 1976.
iii, 42 p. ; 24 cm. (Report - 94th Congress, 2d session, Senate ; no. 94-675)
KF31 .G6 1976

United States. Congress. Senate. Committee on Government Operations. Ad Hoc Subcommittee on Privacy and Information Systems.
Privacy : the collection, use, and computerization of personal data : joint hearings before the Ad Hoc Subcommittee on Privacy and Information Systems of the Committee on Government Operations and the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-third Congress, second session ... June 18, 19, and 20, 1974. Washington : U.S. Govt. Print. Off., 1974.
2 v. (xii, 2335 p.) : ill. ; 23 cm.
Hearings held on S. 3418, 3633, 3116, 2810, and 2542. Bibliography: v. 1, p. 1024-1056.
KF26 .G6586 1974

United States. Congress. Senate. Committee on Government Operations. Subcommittee on Intergovernmental Relations.
Legislative proposals to strengthen congressional oversight of the Nation's intelligence agencies : hearings before the Subcommittee on Intergovernmental Relations of the Committee on Government Operations, United States Senate, Ninety-third Congress, second session ... December 9 and 10, 1974. Washington : U.S. Govt. Print. Off., 1975.
iv, 205 p. ; 23 cm.
Hearings on S. 1547, 2738, 4019, and S. Res. 419.
KF26 .G655 1974c

United States. Congress. Senate. Committee on the District of Columbia.
Wire tapping in the District of Columbia; report. [Washington, 1951]
7 p. 24 cm. ([U.S.] 81st Congress, 2d session. Senate. Report no. 2700)
Caption title.
KF31 .D5 1951

United States. Congress. Senate. Committee on the Judiciary.
Protecting privacy and the rights of Federal employees. Report to accompany S. 782. [Washington, U.S. Govt. Print. Off.] 1970.
48 p. 24 cm. (91st Congress, 2d session. Senate. Report no. 91-873)
Caption title. "Calendar no. 876."
KF31.J8 1970a

United States. Congress. Senate. Committee on the Judiciary.
Protecting privacy and the rights of Federal employees; report to <accompany S. 1438> [Washington, U.S. Govt. Print. Off., 1971]
48 p. 24 cm. (92d Congress, 1st session. Senate. Report no. 92-554)
Caption title.
KF31.J8 1971b

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure.
Computer privacy. Hearings, Ninetieth Congress, first [and second] session[s], pursuant to S. Res. 25. Washington, U.S. Govt. Print. Off., 1967-
v. illus. 24 cm.
Hearings held March 14, 1967- Includes bibliographies.
KF26 .J833 1968c

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure.
Government dossier; survey of information contained in Government files. Washington, U.S. Govt. Print. Off., 1967.
vii, 605 p. 24 cm.
At head of title: 90th Congress, 1st session. Committee print.
JC599.U5 A339

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure.
Government dossier: an inventory of Government information about individuals. New York, Arno Press, 1969.
vii, 605 p. 25 cm. $8.95
Reprint of the 1967 ed.
JC599.U5 A339 1969

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure.
Right of privacy act of 1967. Hearings, Ninetieth Congress, first session, pursuant to S. Res. 25, on S. 928. Washington, U.S. Govt. Print. Off., 1967-
v. illus. 24 cm.
Hearings held Mar. 20 1967-
KF26 .J833 1967a

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure.
Warrantless wiretapping and electronic surveillance, 1974 : joint hearings before the Subcommittee on Administrative Practice and Procedure and the Subcommittee on Constitutional Rights of the Committee on the Judiciary and the Subcommittee on Surveillance of the Committee on Foreign Relations, United States Senate, Ninety-third Congress, second session .... Washington : U.S. Govt. Print. Off., 1974.
vi, 519 p. ; 24 cm.
Hearings held Apr. 3-May 23, 1974.
KF26 .J833 1974

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure.
Warrantless wiretapping. Hearings, Ninety-second Congress, second session ... June 29, 1972. Washington, U.S. Govt. Print. Off., 1973.
iv, 221 p. 24 cm.
Includes bibliographical references.
KF26 .J833 1972b

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Army surveillance of civilians: a documentary analysis. Washington, U.S. Govt. Print Off., 1972.
vii, 87 p. 24 cm. $0.45
At head of title: 92d Congress, 2d session. Committee print. Includes bibliographical references.
JC599.U5 A333 1972

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Criminal justice data banks 1974 : hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-third Congress, second session... Washington : U.S. Govt. Print. Off., 1974.
2 v. 24 cm.
Hearings held Mar. 5-14, 1974, on S. 2542, 2810, 2963, and 2964. Vol. 2: Appendix.
Bibliography: v. 2, p. 1111-1149.
KF26 .J837 1974b

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Criminal justice information and protection of privacy act of 1975 : hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-fourth Congress, first session, on S. 2008, S. 1427, and S. 1428, July 15 and 16, 1975. Washington : U.S. Govt. Print. Off., 1975.
iv, 311 p. ; 24 cm.
Includes bibliographical references.
KF26 .J837 1975a

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Drug abuse data banks : case studies in the protection of privacy / by the staff of the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-third Congress, second session. Washington : U.S. Govt. Print. Off., 1974.
ii, 45 p. ; 24 cm.
At head of title: 93d Congress, 2d session. Committee print.
JC599.U5 U53 1974c

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Federal data banks and constitutional rights; a study of data systems on individuals maintained by agencies of the United States Government: summary and conclusions. Washington, U.S. Govt. Print. Off., 1974.
vii, 53 p. 24 cm. $0.65
At head of title: 93d Congress, 2d session. Committee print. Includes bibliographical references.
JC599.U5 U53 1974

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Federal data banks, computers, and the Bill of rights. Hearings, Ninety-second Congress, first session ... Washington, U.S. Govt. Print. Off., 1971 [i.e. 1972]
2 v. (vii, 2164 p.) 24 cm. $8.75
Hearings held Feb. 23-Mar. 17, 1971. Pt. 2 also has special title: Relating to Departments of Army, Defense, and Justice.
KF26.J837 1971

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Individual rights and the Federal role in behavior modification : a study / prepared by the staff of the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-third Congress, second session, November 1974. Washington : U.S. Govt. Print. Off., 1974.
xii, 651 p. : ill. ; 24 cm.
Bibliography: p. 649-651.
KF3827.B4 A25 1974

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Military surveillance. Hearings, Ninety-third Congress, second session, on S. 2318. April 9 and 10, 1974. Washington, U.S. Govt. Print. Off., 1974.
v, 397 p. 24 cm.
KF26 .J837 1974a

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Military surveillance of civilian politics; a report. Washington, U.S. Govt. Print. Off., 1973.
v, 150 p. illus. 24 cm. $1.50
At head of title: 93d Congress, 1st session. Committee print. Includes bibliographical references.
UB251.U5 U54 1973

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Political intelligence in the Internal Revenue Service : the Special Service Staff : a documentary analysis / prepared by the staff of the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-third Congress, second session. Washington : U.S. Govt. Print. Off., 1974.
xiii, 344 p. ; 23 cm.
At head of title: Committee print.
HJ3252 .U55 1974

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Privacy and the rights of Federal employees. Hearings, Eighty-ninth Congress, second session. Washington, U.S. Govt. Print. Off. 1967.
vi, 966 p. illus. 24 cm.
Hearings held Sept. 23-Oct. 5, 1966. "S. 3779, to protect the employees of the executive branch of the United States Government in the enjoyment of their constitutional rights and to prevent unwarranted governmental invasions of their privacy."
KF26 .J837 1966c

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Privacy, polygraphs, and employment : a study / prepared by the staff of the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-third Congress, second session. Washington : U.S. Govt. Print. Off., 1974.
iii, 18 p. ; 24 cm.
At head of title: 93d Congress, 2d session. Committee print.
JC599.U5 U53 1974b

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures.
Electronic surveillance for national security purposes : hearings before the Subcommittees on Criminal Laws and Procedures and Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-third Congress, second session, on S. 2820, S. 3440, and S. 4062, October 1, 2, and 3, 1974. Washington : U.S. Govt. Print. Off., 1975.
iv, 577 p. ; 24 cm.
Includes bibliographical references.
KF26 .J838 1974

United States. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities.
Intelligence activities : Senate Resolution 21 : hearings before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate, Ninety-fourth Congress, first session. Washington : U.S. Govt. Print. Off., 197
v. : 24 cm.
Hearings held 1975-
KF26.5 .G68 1975

United States. Dept. of Health, Education, and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems.
Records, computers, and the rights of citizens; report. [Cambridge? Mass., MIT Press, 1973]
xxxv, 344 p. 22 cm.
Bibliography: p. 298-330.
JC599.U5 U54 1973a

United States. General Accounting Office.
Need to consolidate responsibility for automatic digital network (AUTODIN) terminals, Department of Defense : report to the Congress / by the Comptroller General of the United States. [Washington : General Accounting Office, 1974]
iv, 53 p. ; 26 cm.
Cover title. "B-169857." Publication date stamped on cover.
UA943 .U54 1974

United States. Library of Congress. Congressional Research Service.
Soviet intelligence and security services; a selected bibliography of Soviet publications, with some additional titles from other sources. Prepared at the request of and based on materials provided by the Subcommittee to Investigate the Administration of the Internal Security Act and other Internal Security Laws of the Committee on the Judiciary, United States Senate. Washington, U.S. Govt. Print. Off., 1972-75.
2 v. 24 cm. $1.25 (v. 1); $4.96 (v. 2)
At head of title: 92d Congress, 1st session. Committee print; v. 2: 94th Congress, 1st session. Committee print. "Organization of Soviet State security:" 3 folded sheets in pocket, v. 2. CONTENTS: [v. 1] 1964-70. v. 2. Covering 1971 and 1972.
Z6724.I7 U54 1972

United States. National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance.
Commission hearings. Washington : National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, 1976.
p. cm. (Supporting materials for the Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance)
Transcriptions of hearings conducted by the Commission and held Sept. 16, 1974-June 27, 1975 in Washington.
KF9670 .A85

United States. National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance.
Staff studies and surveys. Washington : National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, 1976.
p. cm. (Supporting materials for the Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance)
KF9670.A75 N3

United States. Office of Science and Technology.
Privacy and behavioral research.
Washington, For sale by the Supt. of Docs., U.S. Govt. Print. Off., 1967.
v, 30 p. 24 cm.
Commonly known as the Hornig report.
H62 .U54

Usprich, S. J.
The theory and practice of self-regulation : a study for the Privacy and Computers Task Force / S. J. Usprich. [Ottawa] : Dept. of Communications, [1973?]
49 leaves. ; 28 cm.
JC599.C2 U67

Ware, Willis H.
Data banks, privacy, and society / Willis H. Ware. Santa Monica, Calif. : Rand Corp., 1973.
11 p. ; 28 cm. (The Rand paper series ; P-5131)
AS36 .R28 no. 5131 JC599.U5

Warner, Malcolm.
The data bank society: organizations, computers and social freedom, by Malcolm Warner, Michael Stone. London, Allen & Unwin, 1970.
244 p. illus. 23 cm. 60/-
Bibliography: p. 236-242.
JC597 .W37

Wessel, Milton R.
Freedom's edge : the computer threat to society / Milton R. Wessel ; [with a foreword by Paul Armer] ; ill. by Will Eisner. Reading, Mass. : Addison-Wesley Pub. Co., [1974]
xvi, 137 p. : ill. ; 21 cm.
QA76 .W47

Westin, Alan F.
Privacy and freedom [by] Alan F. Westin; with a foreword by Louis Blom-Cooper. London, Bodley Head, 1970.
xvii, 487 p. 23 cm. 63/-
Bibliography: p. 445-458.
KF1262 .W4 1970

Wisconsin. Legislative Reference Bureau.
Privacy: its substance, applications, and legal status. [Prepared by Lawrence Barish] Madison, 1972.
50, [2] p. 29 cm. (Its Research bulletin 72-3)
Cover title. Bibliography: p. [51]-[52]
KFW2420 .L4 no. 72-3 KF1262

Wise, David.
The espionage establishment [by] David Wise and Thomas Ross. London, Cape, 1968.
[5], 308 p. 23 cm. 35/-
UB270 .W56 1968

Wise, David.
The invisible government [by] David Wise and Thomas B. Ross. New York, Vintage Books [1974, c1964]
xii, 378 p. 19 cm.
Reprint of the ed. published by Random House, New York. Includes bibliographical references.
JK468.I6 W5 1974

Workshop on the Data Bank Society, London, 1970.
Privacy, computers and you. Editor: B. C. Rowe. Editorial advisor: Joe Jacob. Manchester [Eng.] National Computing Centre [1972]
212 p. 21 cm. (Computers and people) £3.00
Convened jointly by the National Council for Civil Liberties and Allen & Unwin Limited, and held Nov. 18-19, 1971.
Bibliography: p. 195-201.
JC597 .W67 1970

SUBCOMMITTEE ENCLOSURES

[From the Washington Post, Mar. 16, 1967]

Industrial Spies To Turn to Laser Beam, Computer Snooping

Laser beams and computers will soon replace telephone taps, hidden microphones and the electronic martini olive as devices for industrial spying, a Senate Judiciary Committee eavesdropping expert predicted yesterday.

A laser beam device is being developed that will pick up conversations inside an office via vibrations of voices bouncing off the office's windows, explained Bernard Fensterwald, counsel to Sen. Edward V. Long's Judiciary Subcommittee on Administrative Practice.

The beam could be aimed from a location blocks away from the target office and bounced off the window to pick up the sound vibrations, Fensterwald told a meeting of Electronic Industries Association members.

It could create legal problems for anyone trying to stop the laser beam eavesdropping, he added, since the eavesdropper would not have trespassed physically on his victim's property.

Although details of the laser devices for eavesdropping are being kept secret by their developers, Fensterwald predicted that they "probably will replace many other bugging devices in 10 years."

He also said that the day is coming when some industrial secrets will be stolen via computers. Many firms that have turned to data processing for record keeping are forced by limited finances to share computers with other companies.

Fensterwald said it is "now impossible" to prevent a competitor with access to the computer bank from reading the other firm's stored secrets.

He also warned the businessmen about the many kinds of telephone taps and hidden microphones now in use. One of the most popular, he said, is a transmitter that can be installed "in 30 seconds" in the electrical outlet of any room. It can then be monitored by attaching a receiver to an outlet in any other room in the same building.

Industrial spying is "quite widespread" according to information collected by Sen. Long's Subcommittee, Fensterwald said. He named the natural gas and cosmetics industries as two that are "pretty shot through" with spying.

[From Jack Anderson's column, May 4, 1972 © 1972, by the United Feature Syndicate, Inc.]

Espionage Equipment

American intelligence agencies are perfecting bizarre surveillance devices which make James Bond's gadgets look Victorian.

Some of the equipment is already in use by government agencies engaged in snooping.

The devices depend on lasers, infrared rays and microwaves to eavesdrop, pierce the darkness and peek through keyholes.

The ancient art of training pigeons, for example, has been combined with modern laser techniques. Keen-eyed pigeons have been trained to fly wherever they see a split-second flash of red made by a laser beam.

The beam may be subliminally flashed on the windowsill, say, of a foreign embassy or military conference room. A pigeon, with an adhesive-encased "bug" stuck to his chest, flies to the sill. He is trained to snatch off the adhesive-coated microphone-transmitter, which then drops to the sill.

The "bug" records all conversations in the room. When the intelligence agency wants to retrieve the "bug," it flashes another laser beam. The pigeon flies to the sill, presses his body to the adhesive packet and flies home.

Another laser device simply focuses on a window pane of a room in which people are talking. Their conversation causes minute vibrations of the pane. The pane acts as a mirror, bouncing back the laser beam with an "image" of the vibrations. These are "translated" into voices by a laser receiving set.

Still another eavesdropper floods a room with microwaves and then "reads" the changes in the microwave configuration caused by voices in the room. The Russians used a similar technique successfully against our embassy in Moscow for years.

Lasers have also been developed to heat up a spot on an enemy tank or ship. Then, heat-homing missiles are fired which dart accurately to the heated spot.

Ingenious U.S. infrared experts have fashioned giant searchlights which illuminate whole areas for those with special viewers. The "spotlights" can be mounted on helicopters to reveal troops in pitch darkness. Or they can be set atop buildings to expose the movements of rioters in the dark.

The infrared devices, however, also "illuminate" the dangers of this new family of snoopers. Tests on infrared cameras showed that a 1/1000th flash at 20 feet burned rabbits' retinas.

A former consultant to the Defense Department, Dr. Milton Zaret, has confirmed that the lasers not only bounce off the glass, but penetrate the rooms. The lasers, microwaves and infrared beams can cause cataracts and other long-range injuries to people they strike.

Thus, electronic smog created by the surveillance equipment may be ruining the eyes of spies, Communist diplomats and innocent citizens who just happen to be in or near the rooms when the hazardous rays are unleashed.

[From the Evening Star and Daily News, Monday, Apr. 2, 1973]

That Poodle Could Be a Security Agent

(By Michael Satchell)

Gun-sniffing miniature poodles, bacteria that glow in the presence of weapons or explosives, hidden X-ray and voice analysis machines, and infrared scanners that spot concealed weapons in crowds and instantly pinpoint incoming sniper fire are quietly being developed to improve the protection of the President and other high-level public figures.

Army scientists at Fort Belvoir, Va., began developing the broad range of "Mission Impossible" type devices three years ago, prompted by the assassination in 1968 of Sen. Robert F. Kennedy.

Had such equipment been available earlier, scientists say, there is a good chance that the shootings of Kennedy and Alabama Gov. George Wallace could have been prevented, and that Lee Harvey Oswald could have been captured red-handed in the Texas Book Depository in Dallas after his sniper attack on President John F. Kennedy.

So far, close to $3 million has been spent on the program.

ARMY GROUP CHOSEN

The Countermine/Counter Intrusion department of the Army's Mobility Research and Development Center at Ft. Belvoir was chosen to develop the equipment in the "Protection of Key Public Figures" program because of its experience in detecting mines, booby traps, intruders and concealed weapons.

Details of the Army's research are contained in a paper to be presented by Texford Booth, a civilian scientist heading the program, at an electronic crime countermeasures conference next month at the University of Kentucky.

Advanced metal detection equipment already has been widely tested at Washington's National and Dulles Airports, at Chicago's O'Hare Airport, and at the District of Columbia jail where persons visiting inmates have been electronically frisked. The jail equipment recently turned up two smuggled weapons, and court cases are pending.

These devices, known as active or passive magnetic portal detectors, are advanced versions of the walk-through columns familiar to air travelers. Tests so far have resulted in a detection rate of 99 percent for .32-caliber weapons or bigger, and 89 percent for the less bulky .22- or .25-caliber guns. The false alarm rate—caused by keys or belt buckles is less than 10 percent.

X-RAY EQUIPMENT

This advanced type of weapon detector forms the basic unit for protecting the President or public official in a controlled access situation and they can be built into an entranceway and disguised without problem.

In a situation where permanent maximum security is needed—say the East Room of the White House where the larger functions are held—additional refinements currently being developed could be added to the basic detector unit.

Complex hidden X-ray equipment built around a revolving door could be used to give a person a full body X-ray if a detector indicates he is carrying a large mass of metal, possibly a weapon. A hidden operator could confirm at a glance whether a gun is concealed. In a White House situation, such surreptitious screening could avoid potentially embarrassing body searches, especially if high-level guests are involved.

To the metal detector and X-ray machine would be added a Psychological Stress Analyzer. Picture a situation where the East Room is packed with dignitaries and the Secret Service is suspicious of an individual. The agent, after presumably maneuvering the suspect within range of the analyzer, could ask a few harmless questions about the weather and such, and the replies would be recorded and automatically analyzed.

The equipment would sense the stress level in the voice. Ft. Belvoir scientists say they expect to be able to produce a stress analyzer that could interpret whether a person is simply worried about an outside, personal problem or whether he is about to commit an act of violence.

Spotting hidden weapons or explosives along a motorcade or at a large gathering is much more difficult. The Army researchers are working on a variety of approaches including trained miniature dogs, large infrared crowd scanners and various, handheld devices that would be carried by agents mingling in the crowd.

They are being taught to sniff out guns by learning to detect the scents of gun oil, gun solvent cleaner and the powder residue left in the barrel and chamber after the weapon is fired.

Small dogs, including miniature greyhounds and poodles, pomeranians and whippets are presently being tested and trained at the Southwest Research Institute at San Antonio, Tex., under an Army contract.

"Police-type dogs such as German Shepherds would be too obvious and would also have difficulty circulating in a big crowd," a scientist said.

"We chose miniature dogs because they can be handcarried into a crowd. And what is more natural than to see a woman—a security agent in this case—carrying her miniature poodle?"

Another researcher said whippets and miniature greyhounds have so far proven the most adept at detecting guns. "They have tremendous curiosity, and they have nice long necks to reach out and sniff inside someone's coat," he said. All the dogs being tested in the secret study are spayed females thus one potential distraction from their work is avoided.

METAL DETECTORS

Also circulating in the crowd, according to the Army scenario, could be plain-clothes agents carrying briefcases containing miniature metal detectors based on the same principle as the doorway type devices.

The agents would be equipped with special spectacles containing a tiny radio receiver, probably tucked behind the ear like a small hearing aid. When the briefcase device detects a weapon, it would send a radio signal to the spectacles which in turn would sound a tiny beep in the agent's ear.

Even more fanciful hand-carried devices are being developed including trace gas detectors, small units about the size of a pocket calculator containing bioluminescent bacteria that glow when they sense certain gases given off by explosives.

The Ft. Belvoir scientists are also attempting to develop strains of bacteria that react to gun oil, solvent and powder—the same elements that the dogs are being taught to sniff.

SNIPER ATTACK

While agents are mingling with the crowd in the search for potential assassins, a large device called an infrared imaging system—mounted on a truck or possibly into a speaker's podium—would be scanning the crowd close to the stage.

Much like a television camera that zooms in to focus on a face in a crowd, the infrared scanner could zero in on an individual and by reading the infrared energy radiated from his body, could discern the shape of a concealed weapon.

The technique is being adapted from systems currently used by industry to detect flaws in parts coming off an assembly line, or by medicine in detecting hidden cancers, the Army developers say.

In the sniper attack situation, an infrared gunflash detector under development would be built into a vehicle for use in a motorcade, or parked near a large gathering.

The equipment would sound an alarm when a sonic sensor detected an incoming round within 50 feet of the device and a readout diagram would show the operator virtually the exact spot from where the rifle was fired.

[From Jack Anderson's column, Friday, May 4, 1973, © 1973, United Feature Syndicate]

Migraine weapon.—Confidential plans are now under study for a riot-control machine which sends out beams strong enough to give "migraine-like headaches." This futuristic weapon, proposed by advanced Pentagon scientists, is aimed at replacing "rubber bullets . . . electrical prods, dogs, gas, water and clubs" as a riot-dispersing device. Still in the design stage, the system would use sensors and computers to make sure that only the rioters get the full blast of head-splitting sound which would range from noiseless high frequency beams to a racket intended to drown out agitators. The proposal is called "non lethal," but the confidential documents describing it warn that sound machines must be carefully developed to prevent "catatonic fits in schizophrenic individuals" or even death.

[From the New York Times, June 20, 1973]

Police To Use TV To Scan Times Square Area for Crime

(By Murray Schumach)

A crackdown on crime in the Times Square area through the use of closed-circuit television is due to begin next month. Under plans being made by the Police Department, the television eyes for the Great White Way and its side streets will be set up with the arrival of a police trailer in the Times Square area. The trailer will have television screens.

Details of the camera surveillance are being withheld. Police Commissioner Patrick V. Cawley declined to comment, and it could not be learned how many cameras would be used, where they would be placed and which streets would be showing up on the screens in the trailer.

PROTECTION FOR TOURISTS

The general belief in the Police Department was that the trailer would be between 43d and 44th Streets in the Times Square area.

The trailer, which is expected to be in operation as the summer wave of tourism hits the city, will be similar—except for the television screens—to one now situated in the garment center and called a "subprecinct."

From the van, the police will be able to direct, by radio, assistance to the scenes of crimes or apparent danger.

"I think every law-abiding person who comes to the Times Square area will be delighted to know he is being protected in this way," said Deputy Inspector James E. Dicks of the Midtown South Precinct. "Only criminals will be worried about being on this television screen."

Inspector Dicks, whose manpower has been strained in spite of reinforcements from other precincts, said he did not know how many television eyes would be set up or which blocks would be under surveillance.

BLOCKS TO BE VIEWED

"We do know we will be able to have entire blocks under television watch," said the inspector. "I can't help feeling that business will fall off for prostitutes when the Johns realize they may be on television.

"If the hooker can't make money, she goes away. And if she goes, the pimp goes. And the narcotics pusher goes. And the whole setup that feeds on this kind of world has to move elsewhere."

The inspector was hopeful that the television watch on the streets would also tend to discourage muggers.

"We need this technological help," said the inspector. "You can't put a policeman in front of every doorway. So far as I know, no major city has used this system against crime. We hope to be the front-runner.

SYSTEM TRIED UPSTATE

The system was tried experimentally in Olean N.Y., during the late nineteen-sixties. Police Chief Michael S. Luty said yesterday that he thought it had worked well and was "a good crime deterrent." However, it was opposed by the successful candidate for Mayor, William O. Smith, who considered it an invasion of privacy.

Two television cameras are in use in Mount Vernon, N.Y., on top of light poles on Fourth Avenue. One is at First Street and the other at Second Street.

According to the police in that city, the cameras are crime deterrents. Federal grants paid for the cameras, they said.

It could not be learned here yesterday whether the money to purchase or operate the Times Square television devices would be from the Federal Government.

Mayor Lindsay, in a recent announcement of a city plan to finance anticrime campaigns by block associations, tenant groups and similar organizations, did not mention television surveillance. However, others in the city government said this was one idea under serious consideration, coupled with Federal support.

The New York City Police Department, during the period of frequent demonstrations against the war in Vietnam, occasionally used television to help officers direct police tactics. The cameras were placed on roofs or in the windows of upper floors of skyscrapers.

One of the areas frequently under closed-circuit television then was City Hall Plaza. Police officials said yesterday that this kind of surveillance was abandoned a couple of years ago.

Of the system planned for Times Square, Inspector Dicks said:

"This will give us real directed patrol."

[From the New York magazine, July 9, 1973]

NEW YORK

Wired City: The Invasion of the Privacy-Snatchers

By Thomas Plate

"...Last year some 6,500 New Yorkers were the targets of court-ordered wiretaps. So much for the figures on *authorized* taps..."

New York is Wired City. This is the city of tapped candy-store pay phones, bugged board rooms and wired political clubhouses. This is the city whose wire-and-bugmen are so hip that they scoff at the Watergate plumbers the way seasoned hitters smirk at a young rookie taking his first cuts at a major league curve ball. This is the city where the stakes are so great—fame, fortune, marriages, careers—that you'd have to be pretty naive to assume there's nothing going on. "I haven't used my telephone for business in 25 years," a top mobster told men from the Brooklyn District Attorney's office recently. "I only talk in code now," said a well-placed Democrat in town. "I never speak openly on the phone."

New York is full of individuals who feel a vested interest in their neighbor's business. There's a major branch of the Federal Bureau of Investigation over on East 69th Street, and you know what they do. There are all those United Nations delegates around town, and you know what many so-called "cultural attaches" get into. Then you have Toy Company X shelling out several grand a month to Fast-Buck Electronics to get a line on Toy Company Y's Christmas marketing plans. You've got Charlie Cuckold retaining Seedy Detective Agency to wiretap the wife's phone. You've got five crime families running around town, mobbing businesses up and gunning competition down; gambling rings quietly taking in millions of dollars of illegal bets daily; narcotics wholesalers bringing the stuff in and distributors cutting it up and getting it on the streets; smugglers and hijackers emptying planes and trucks, and fences moving the goods out. So you've got Federal, state and local law enforcement officials running around town listening for leads, gathering evidence of conspiracies, and hoping for the best—that is, the worst.

A good deal of the tapping and bugging in Wired City is legal, and accounted for. There are precise numbers in the files of those law enforcement officials who, under Federal and state law, go to judges for authorization of their wiretapping or bugging plans.

There were, for starters, 294 separate authorization orders signed by state judges in New York in 1972, representing 45 per cent of all orders signed by state judges *nationwide*. Of the state's total, New York City accounted for 52 per cent—or 23 per cent of the total nationwide.

Some 6,500 New Yorkers last year helped make New York number one in electronic surveillance.* These are the obvious criminals, assorted suspects, and mistaken identities who were the targets of those court orders.

So much for the figures on authorized tapping. Worrisome as it is, it is the *unauthorized* tapping and bugging that has many New Yorkers uptight.

"There is probably a good deal of illegal wiretapping in New York," says Eugene Gold, the Brooklyn District Attorney. "In my judgment, the vast majority of it is done by private firms for private businesses." Gold's assessment tends to support the view offered by Samuel Dash, now majority counsel of the Senate subcommittee investigating the Watergate scandal, in a book published more than a decade ago. "It is safe to say," wrote Dash in 1959, "that most of the private wiretapping done in the world is done in the City of New York."

There are about 130 private investigative firms in Manhattan borough alone. Most of these are strictly on the up-and-up, which is only to say that most of them don't commit felonies like wiretapping. But some are not. Pete Andreoli, the head of the Supreme Court Bureau in District Attorney Frank Hogan's office, says that while most of the shady, bug-prone operators have been moved out of Manhattan, you can still get a tap put on a phone if you pay the market price, which can be quite stiff (if for no other reason than overcharging is quite common). Despite the cost, private enterprise accounts for most of the illegal wiretapping in the city.

Most, but not all. Some illegal wiretapping is no doubt done by overzealous law enforcement officials who won't wait for a court order to nail some crook.

"Any good cop, any good detective," says a former state rackets squad investigator, "will extend himself a little.

*A single court order can authorize electronic eavesdropping on more than one suspect. Indeed, that is invariably what happens, at least in New York. Last year, according to data provided by the five D.A.s, 155 orders were issued in New York City. Each order on the average involved the overhearing and recording of conversations in which roughly 30 people took part. By such arithmetic (30 x 155), and adding on the number of persons tapped by the two United States Attorneys with jurisdiction in the city, we estimate New York's legally bugged population for 1972 at 6,500—minimum.

The essence of the bug is miniaturization: *The largest of these three dynamic mikes is a standard stage mike, the other two sensitive bug-mikes that can be hidden under a chair or in a telephone to effectively pick up any conversation in the room.*

Photographed by Steve Myers

It's only human. You justify it in your mind by saying you're not breaking any moral law, you're after criminals."

But there is ample reason to fear that illegal wiretapping is also done by some lawmen simply doing a little mean business on the side. Electronic surveillance is a powerful weapon, and, in the hands of an unscrupulous cop, can be used as a machine for coining money. As one Government investigator told me recently (for obvious reasons he didn't want his name printed): "Look at it this way. Suppose you're a crooked cop and you know Joe Blow over on 125th Street is probably pushing narcotics. On your weekend off, without telling anybody, except maybe your buddy who's in on the deal, you put a tap on this guy's phone. Then, on Monday, you take the tape off the recorder in the guy's basement and go have a nice little chat with Joe the Pusher. You tell him this interesting little tape was dropped into your hands by a little birdie and that you want to be careful with it because you don't want it to fall into the wrong hands. Like the District Attorney's."

It happens. It probably happens less now than it did as recently as three years ago, if only because of the heat generated by the Knapp Commission and by high-ranking police officials under the Murphy-Cawley administrations—not to mention all the Watergate publicity which has undoubtedly heightened public concern with bugging. But still, things happen. In his landmark study of electronic surveillance entitled *Eavesdroppers*, Sam Dash claimed that New York city police have been tapping phones illegally since 1812, when illegal phone taps were first made a crime in New York State. In his book, Dash developed a method for estimating the number of illegal taps in place on the basis of the known legal ones. Dash took a number of variables into account, including the number of ex-telephone company workers on the police force. Out of all this arose the so-called Dash Rule, which holds that in a large metropolitan police force like New York's, the ratio of illegal taps to legal may go as high as nine to one.

Some experts think the amount of illegal taps is overstated but a lot of people in high places in town behave otherwise. Governor Rockefeller's phones, for example, have been regularly "swept" ever since state police officials discovered, six years ago, a tap on Rocky's office phone at West 55th Street. The city's five D.A.s take no chances either. Nor do CBS and NBC, which regularly check the phones of their top executives for tampering. And the Special State Prosecutor, Maurice H. Nadjari, has his offices in the World Trade Center swept for taps and bugs about once a week, even though, as his chief investigator Joe Feeley put it, "If somebody really wanted to put a bug in here, and knew what he was doing, he could probably get away with it."

Nadjari himself has been accused of wiring the city like a berserk spider weaving a complex web. Howard Samuels, the Off-Track Betting boss, who has plans to run against Nelson Rockefeller next year, is concerned that there may have been taps on his phones, and worries that perhaps Rockefeller-appointee Nadjari might have been behind them. In Samuels's case, there seems every reason for concern. John Cye Cheasty, a private investigator hired by the O.T.B. people to sweep phones and rooms for taps or bugs, told me that he found remnants of what was clearly a very sophisticated tap on a phone in Samuels's apartment on Manhattan's East Side last month. Nadjari's people take the position that any insinuation that they are bugging Samuels is beneath comment—the only persons "being bugged by this office are people suspected of committing crimes," said a spokesman. Nevertheless, Samuels's people remain suspicious. So do a group of Queens judges, who have been complaining that their phones have been tapped, and who suspect that Nadjari is behind these as well.

Several years ago a pretty good film made the rounds called *The Anderson Tapes*, starring Sean Connery. The film's premise was that there is a hell of a lot of wiretapping going on in New York but that the agencies doing it don't know what other agencies are doing. "That film was probably the worst thing that ever happened to law enforcement as regards wiretapping," Nadjari said recently. "It suggested that we were all running around in a bumbling way." It could be. One highly regarded wireman in the Bronx District Attorney's office tells of an investigation last fall at an address on the 100-block of East 68th Street.

"First thing I figure is, better tell the F.B.I. [whose office is at 201 East 69th]. After all, we're going to be in

The Wiretappers

Law Enforcement Office	Number of Persons Overheard by Taps (Estimated)	Number of Orders (January 1, 1972 December 31, 1972)	Violation Most Often Cited to Justify Wiretap	Average Cost Per Court Approved Order	Phone Taps As a Per Cent of Total Electronic Surveillance[2]
The City's D.A.s					
Bronx	640	43	Narcotics	$10,364	87%
Brooklyn	420	50	Narcotics	11,451	97%
Queens	795	28	Gambling	N.A.[3]	80%
Manhattan	2,232	128	Narcotics	5,585	74%
Staten Island	136	5	Gambling	6,764	100%
U.S. Attorneys[4]					
Eastern District (includes Brooklyn, Queens, Staten Island)	1,116	15	Gambling	N.A.	N.A.
Southern District (includes Bronx and Manhattan)	909	10	Gambling	N.A.	N.A.
Federal Bureau of Investigation	N.A.	N.A.	National Security/ Interstate Thefts	N.A.	N.A.
Special State Prosecutor (Maurice H. Nadjari)	N.A.[5]	N.A.	Conspiracy/ Corruption	N.A.	N.A.

[illegible] interceptions [illegible] several [illegible] conversations [illegible] conversations [illegible] a phone in a [illegible] market used [illegible] to arrange narcotics transactions [illegible] are [illegible] a pay phone. But [illegible] are [illegible] at their present level 1971 [illegible] totals.

[illegible] to car buffs, room bugs, and the like

N.A.—Not available

[illegible] for example, such Federal agencies as the Bureau of Narcotics and Dangerous Drugs and Customs which turn over investigations to Federal attorneys for indictment.

Officer is [illegible] by Administrative order on 9/19/72, currently banned to [illegible] taps or bugs in operation. Nadjari's petition for the [illegible] our evidence must be authorized by Attorney General Lefkowitz before they are sent to State Supreme Court Justice John Murtagh for approval. Lefkowitz himself has no powers of criminal prosecution. New York is one of the very few states in the union whose Attorney General has [illegible] as opposed to criminal, prosecutorial powers.

the basement almost around the corner and we don't even mention it? So I pick up the phone and tell them we're going to put a tap on a phone 'pair' [illegible] connects a given phone to an [illegible] in an apartment nearby.

"So this guy over there checks around and says, 'Okay, go ahead, no problem.'

"Next night we're in the basement of the building. One of the guys opens the bridge box and the next thing we hear is, 'For the love of Mike, will you look at this?'"

The technician pointed to a red seal covering another pair—not the one the D.A.'s men were planning to tap, but one for a phone in the very building they were in. The wiremen were understandably startled because on the red seal were the words "Presidential Authority." They had never seen a seal like this before.

"But by this time we figured, what's one seal to us? We're tapping a different phone. So we go to work. But then who should come through the door—I'm telling you it was some night—but this blonde. And she's fit to be tied. I'd guess the doorman tipped her off that we were down there."

The city's experienced wiremen rarely if ever tell doormen what they're up to. Invariably they enter a building in one disguise or another—as boiler repairmen, phone company technicians, even, yes, as plumbers.

"So this blonde wants to know why we're tapping her phone, the one with the red seal on it. We tell her we're from the D.A.'s office, we're not tapping her phone, but someone else's, and we have a court order, which we show her. She leaves but she's not too happy about it. We stay and install the tap.

The next morning, back in the office all hell breaks loose. The Secret Service calls us and they're not very happy. 'What the hell were you doing in that building? Don't you know that girl is a friend of Henry Kissinger's and that red seal covers a special Government phone line?'

"Well, we didn't know that the blonde was Nancy Maginnes, and that sometimes she has a male caller named Henry Kissinger, and that sometimes he uses a special phone in her apartment to call Washington. And we told the Secret Service just that—and we told them it wasn't her phone we were tapping. Eventually they calmed down.

"But by this time I'm wondering why the F.B.I. didn't tell me anything. So I call my friend over there and say, 'Why'd you set me up like that?' And they answer—and I still can't believe it—'We didn't know about it. We didn't know he visits there.' Can you believe that? Can you imagine that?"

"That red seal," says Jack Miller, supervisor for the New York Telephone Company's security department, "was not a tap. It was simply a warning to our men not to mess around with that pair. It tells us that this is a special line. In fact, it's probably a Western Union line that goes directly to Washington."

Any law enforcement official in town who has anything to do with wiretapping knows Jack Miller. He is the phone company's main man on such delicate matters as wiretapping. If a wireman needs to know where the best places are to tap a phone, he will contact Jack Miller. If he's got a court order, Jack Miller will help. If he doesn't, Miller says he won't. But sometimes a wireman won't head for the phone company even when he has a court order. For the phone company has had its own security problems. In one memorable instance, nearly a decade ago, a telephone employee was considered to be on the take from the mob. Every time the cops tried to put a tap in, the Brooklyn mobsters affected by the court order suddenly stopped using the phone. Eventually an official inside the phone company was fingered, and he quietly left the company. Now no one in town is alleging that there are such corrupt employees at New

The complex art of debugging: *Here a telephone company investigator takes apart a phone at "New York" Magazine in quest of a hidden bug or tap. He found none.*

York Tel today. Especially Jack Miller, who is regarded by the town's law enforcement officials as tough, honest and straight. But to get the phone company's cooperation on a tap, a lot of people have to see that court order. Sometimes, apparently, it's not worth the risk, however slim.

Even when the risk is taken, Jack Miller is understandably stinting with his help. He'll give a D.A.'s wireman the "schematics," as the necessary diagrams are called, to a circuit, but he won't help them put in the tap. (Last year the phone company "responded" to 176 requests for such assistance.)

The phone company is much more cooperative when a customer suspects a wiretap on his line. Last year more than 2,000 customers in the city contacted New York Tel to register that fear. Miller says he checks out every complaint.* "Most of them hear static on their line," he says. "Now if you hear static, you know the job's not being done by a professional. Actually, what you really know is that there's something wrong with your line, like water erosion, having nothing to do with wiretapping." And, to make matters worse, many customers pass along their complaints over the very phone they thought was tapped. "Now that's just plain dumb," says Jack Miller. "Nobody running an illegal tap who hears that person call is going to wait around for us to come and establish that they're committing a felony." The vast majority of the complaints Miller and his men receive don't check out—maybe four or five a year are forwarded to the D.A.'s office. "It seems that every time the moon is high, or you have something like this here Watergate," he says, "we get overwhelmed with complaints."

After the line is checked out thoroughly by technicians, the phone company gives you one of three official responses. If there is absolutely nothing on your line, you are told that it's clear. If there's an illegal tap or wire on your line, you're told that the District Attorney has been informed of the matter. The third response, however, is the tricky one. If there is something on your line—*and* it is there because of a court order—then you are told that there is no illegal tap on your line—and under law the phone company is prohibited from divulging the existence of a court-ordered wiretap. "When the tap is legal, under state law we really can't tell you anything," says Jack Miller.

It is not an easy position to be in. "This is the gray area," says George Ashley, the phone company's general counsel. "This is the part that gives us the most trouble. We're put in a box. The statute prohibits us from disclosing the existence of a court-ordered wiretap. But, at the same time, we have an obligation to our customers to provide them with service and privacy."

The phone company is in an even more compromising position when it comes to dealing with F.B.I. requests. As it now stands, the phone company will assist Federal agents upon receipt of a letter signed by the Director of the Bureau invoking "the specific authorization of the Attorney General" and indicating that the tap is a "necessary investigative technique under the powers of the President to protect the national security." In short, the phone company takes the F.B.I.'s word that the tap is justifiable under national security grounds. It does not question the F.B.I. as to what it means by the phrase "national security." It does not, like the Supreme Court in its ruling on June 19, 1972 (*United States v. United States District Court and Judge Damon Keith*), require that the Federal Government distinguish between *foreign* national security saboteurs and *domestic* saboteurs, the latter, under this historic ruling, requiring the F.B.I. or any other Federal agency to obtain a court order for the tap just like everybody else. "We have to *assume* that the Attorney General is acting in accordance with the Supreme Court ruling," says George Ashley, with commendable candor. "Nevertheless, the fact that this power could be abused by them in their dealings with us is there."

The phone company, in effect, is forced to walk on thin ice. Although it is pledged to serve its customers, it is compromised by legal statutes and feelings of patriotism. "But we don't be[lieve] you," insists William Ellinghaus, president of New York Telephone. "By keeping quiet after you request us to tell you whether your phone is tapped, it seems to me that the customer ought

*At our request, his men checked out "New York" Magazine's editorial and business offices on East 32nd Street last week. Complete with sweeping gear and all, three telephone company investigators checked our phone lines and offered a few pointers. Among them: keep the basement pair box under lock and key.

Photographed by Herb Gora

"... Law enforcement officials are pretty candid about wiretaps and bugs. They are sorry that they can't use more of them ..."

felt wasn't tapped. But the cops could never be sure he'd use that phone. One day the gambler made his usual tentative call from the Third Avenue bar two blocks away, emerged from the bar, and began to look around for a pay phone on Third from which to call Miami for the real business conversation. But every pay phone on the avenue had an out-of-order sign on it. So the gambler went into the Old Seidelburg. There was no out-of-order sign on that one. This gambler is now serving a four-year prison term. "All we did," recalls one of the investigators, "was to go around Third Avenue putting up out-of-order signs on pay phones."

Some cops will do anything to get a criminal to use the phones.

Everybody's understandably edgy about wiretapping now, even those doing it. "It can be a real dirty business," says Mario Merola, the Bronx District Attorney. "For me, the whole concept is nauseating."

The unknowns are the stuff of bad dreams. How many lease-lines run from private phones to F.B.I. installations around town? No one knows. (Phone company sources say "the number is very small, less than a hundred.") How about C.I.A. bugging and tapping? The C.I.A., which has a major base in midtown Manhattan, is not supposed to bug United States citizens in this country, but by the same token the Nixon Administration wasn't supposed to tap Daniel Ellsberg either.

Nobody, in short, knows for sure who is doing what in Wired City. Not the phone company, which only knows what it is told. Not Sam Dash whose book alleging widespread illegal use of wiretaps in the New York City Police Department remains necessarily a statement of unverifiable suppositions. Perhaps not even the law enforcement establishment in town, where the left hand doesn't know—because it *can't* know—what the right hand is up to. ■

The Bugs and Wires of New York

Many New Yorkers, especially judges, think of bugs and wiretaps as pretty much the same thing. They're not. A wiretap is an electronic device that picks up both ends of a telephone conversation—long distance as well as local calls. Bugs detect voices in a defined space—a room, a car, the area directly around a corner mailbox. The legal constraints on the two differ as well: protection from bugging is based on the Fourth and Fourteenth Amendments, from wiretapping on the Federal Communications Act of 1934. But Federal law authorizing both is based on the same statute: Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

There are several sorts of wiretaps. You have, for starters, the so-called *parasite* wiretap. This is a miniature transmitter which is literally wired into a telephone line. The good thing about this little device—some are as small as a fingernail—is that it draws the power it needs from the telephone company's line itself. "But the bad thing about these parasites," says a city wireman, "is that the next-door neighbor might pick up the transmitter on an FM radio. Their frequency is uncontrollable."

Another type of wiretap is the *parallel parasite*—a microphone and transmitter combined that comes complete with its own little battery. The battery doesn't last very long, but when it runs low the gadget's circuits permit it to get recharged from the juice on the phone line itself. In this way, you can leave a parallel parasite on a phone line for quite a while.

A third type of wiretap is an *induction coil* device. This gadget draws power from the electromagnetic waves generated by the operation of the phone. But induction coil wiretaps are crude. It's hard to control their frequencies and keep them from running amuck and getting picked up on a total stranger's radio.

The simplest wiretap system of all is the most common: a direct tap right on your phone pair in the phone company's very own bridge box (generally in the basement). A technician simply hooks a set of wires onto your pair and runs them into a tape recorder and/or a headset hidden somewhere nearby.

Bugs, in comparison, tend to be much more sophisticated—and unreliable. Bugs work three different ways: they can transmit from, say, your bedroom just like a little radio station; or there can be a little microphone in your den, to which is attached a wire running to a tape recorder or a headset; or, finally, an agent can point an amplification mike through an open window and pick up your conversation—like NBC-TV aiming a mike at Joe Namath barking signals on the field and picking up his voice although the mike is on the sideline yards away.

Bugs are appropriately named: they are small, self-contained, and ugly. One of the most ingenious kinds now loose in Wired City is the *harmonica* bug. This little devil can be put inside the body of your phone—or connected to it with a wire. It doesn't do anything (except suck a little current out of the phone company's circuit) until its owner literally blows the whistle. It works like this: the bugger (the person who planted the device) picks up any phone, anywhere in the United States, and dials the number of the buggee (the victim). Even before the victim's phone rings the first time, the bugger blows a certain note into his end of the phone. He can, if he wants, use the high note on a standard harmonica (hence the name) if the bug is set for that frequency. Once the harmonica bug is activated, the bugger sits on the other end of the phone line, listening to every word in the buggee's room. "There are only two disadvantages to this kind of bug," says one undercover wireman in the Manhattan D.A.'s office. "The first is that if the victim tries to make a call on his phone [while the bug is activated], he won't be able to get a dial tone, so you've got to get off the line fast when he picks up. The second disadvantage is that the bugger has to pay for the call."

Other kinds of bugs: the *voice-activated* bug, which starts up, and draws energy from a self-contained battery, only when someone talks; the *AC intercom*, which is nothing more than a conventional intercom small enough to hide; the *AC transmitter* (usually a bug hidden in an electrical outlet which draws power from your line, or in an electric socket, activated only when someone comes into the room and turns on the light); and a *spike bug*, an old device, which pierces a wall and permits the Listening Tom to hear a conversation in the next room.

Two pieces of advice from the city's law enforcement wiremen to would-be users of bugging or wiretapping equipment. First, the use of this kind of equipment, if the intent is criminal, is a felony under state law. Second, most of the free-lance wiremen and bugmen around town are hacks (or "mechanics" as they are termed in the trade). You can probably count the total number of truly sophisticated wiremen in this town on the fingers of three hands. And, third, most private-detective firms and electronic outfits vastly overcharge for their services and equipment. Besides which, the truly unscrupulous one will try to keep you as a client once you are hooked. "You can never get a guy," says Manhattan Assistant District Attorney Pete Andreoli, "to make him believe his office is tapped when there's nothing in there." —T.P.

[From the Washington Star-News, July 29, 1973]

Young's Federal Spotlight—52 of 60 U.S. Agencies Reported Using Bugs

(By Joseph Young)

The White House is not the only place where conversations have been bugged by electronic devices.

Virtually all other government departments and agencies have similar equipment to record telephone conversations, many times without the knowledge or consent of those involved. However, the kind of sophisticated equipment that was used in President Nixon's White House Oval Office and at Camp David to record non-telephone conversations is very rare in other government agencies.

The weekly publication, Federal Times, reports that government agencies spent about $137,000 last year on electronic listening-in gadgets. These include tape recorders, wired-in to telephone circuits and special "push-to-talk" telephones that are rented from the telephone company.

Federal Times' staff writer, Court Gifford, reported that although federal regulations prohibit the "installation of listening-in circuits, transmitter cut-off switches and other devices for recording and listening to telephone conversations, most agencies use them anyway.

The $137,000 spent last year by government for electronic listening-in devices is over and above that already spent in previous years for such equipment.

The House Foreign Operations and Government Informations subcommittee in 1970 issued a report that warned of "a dangerous drift toward a huge bureaucracy peering over the shoulder of the citizen."

A survey of 60 federal departments and agencies in 1970 showed that 52 permitted monitoring in some degree and the cost of equipment rental was running about $137,000 a year, the subcommittee reported.

Despite the subcommittee's findings and criticism in 1970, it apparently didn't deter the departments and agencies which continued to spend about the same $137,000 a year for additional electronic listening-in devices. Subcommittee sources say this is an indication that the practice has increased since 1970.

[From the New York Times, Oct. 14, 1973]

'Eye in the Sky' Cuts Kansas City Crime

Kansas City (AP).—"Beep!" . . . "Beeeeeep!"

The double tone on the police band radio signals the two patrolling officers that an important message is about to be relayed.

"All units in the central zone: A bank alarm has been tripped at 12th and Baltimore. Units in the area, please respond."

The officer on the left of unit N9522F swings the vehicle toward the address while the man on the right scans the ground, looking for unusual activity like a speeding car.

It is a routine police response to an alarm. Except that N9522F is a Hughes model 300 helicopter cruising at 50 miles an hour 500 feet above the city and the officers form the Sky ALERT patrol, whose territory is the entire seven-county metropolitan area.

ALERT is an acronym for Aerial Law Enforcement Response Team. Areas that it regularly patrols showed a 26 percent drop in crimes last year and the patrol is credited with being a significant factor in the city's 11 percent decrease in crime.

AVAILABLE AT ALL TIMES

The city, which was the first to have a regular helicopter patrol, has six Model 300's in its fleet and one is available 24 hours a day.

Commander of the unit is 39-year-old Capt. William H. Moulder, who was one of the original members of the force chosen to become a helicopter pilot in early 1967. None of the original three had previous flight training.

There are areas with high crime rates that are patrolled regularly, while other areas receive infrequent checks, Captain Moulder said.

The unit has 11 pilots, including four supervisors and 11 observers. A pilot and an observer are teamed and, just as in patrol cars, work together all the time both are assigned to the unit.

A pilot-observer's eight-hour shift is broken up into four parts: two hours flying, two hours on the ground, two hours flying, two hours on the ground.

PAPERWORK ON GROUND

When on the ground, the men fill out reports, study lists of stolen cars, read data and perform other duties related to work.

To get into the unit, a member of the regular police force must apply and be placed on a list to become an observer. To be eligible, he has to have at least two years on the force and not more than 15.

A man must be an observer at least one year to become eligible to be a pilot. Upon appointment as a pilot, a man is sent to California where he receives 40 hours of flight instruction and returns to Kansas City for the remainder of the 150 hours needed for a commercial license.

Observers also receive special training.

The salary range for a pilot is $13,250 to $13,908 annually; an observer is paid the same as a patrolman, $8,988 to $12,612.

Last year, the unit logged 5,974 hours in the air, 5,550 on patrol. Helicopters also are used in test flights, surveillance, photo flights and demonstrations. Crews aided ground units more than 7,000 times on car checks, robbery and burglar alarms, car chases and other things.

The helicopter is called on frequently at night because it is equipped with lights that generate 1.2 million candle power.

Long-time members of the unit stress that the helicopter is just a tool in the police arsenal and they are there only to assist the officer on the ground.

[From The Village Voice, Oct. 18, 1973]

Voiceprints—Your Fingerprints Belong to You, But What About Your Voice?

(By Larry Lee)

San Francisco.—Ernie Nash is a peculiarly modern success. First he was a television repairman. Then he entered the Navy and got the free training which led to a well-paying civilian job in a growing field, police work.

Today, at 43, Nash is a detective lieutenant in the Michigan State Police, the chief of a lab full of spiffy gear. He has enough spare time to work on getting a college degree, and he has the blessings of his superiors in his ceaseless travels as America's number one prosecution witness on acoustical spectrography.

Ernie Nash prefers to call his job "voiceprint identification," a term genericized over the past 11 years through its use by fictional characters in "Dick Tracy," "Ironside," and "2001."

The real-life voiceprint future Nash and his colleagues talk about looks like this:

Credit access through a nationwide voice verification system. (AT&T. Patents. Working lab models.)

Submission to recording of "voiceprint exemplars" by job applicants. (Under consideration by a large American corporation counseled by Nash.)

A voiceprint criminal identification system designed to use short, sharp utterances from "uncooperative suspects." (Preliminary work under way by North American Rockwell under a grant from the Law Enforcement Assistance Administration. Proposed voice population for lab tests: "minority males.")

All these ideas contain the notion of sending people to jail through the sound of their voices and the hope that some day computers will be able to perform voice verification and identification in a reliable way. So far, the computer experts report only limited success.

Nevertheless, people have gone to jail, thanks to, more than anyone else, Ernie Nash. He has helped with more than 40 of the 51 known voiceprint prosecutions and reports that most have ended in convictions or bargained pleas of guilty.

Nash's pocket calendar is full of future courtroom dates, and he says he likes the travel part of his job. His favorite place so far has been Hayward, California, a suburb of Oakland, "because of the people there."

Ernie Nash is not a villain. He is the software.

When it all began years ago, the software was in the head of Larry Kersta, a Bell Labs scientist who printed a paper in "Nature" suggesting a rather precise corollary between fingerprints and acoustical spectrograms.

Fingerprints appear to be everything we were told they were during our childhood tours of FBI headquarters—in some cases, evidence weightier than eye-witness testimony. Acoustical spectrograms, on the other hand, are an old tool of speech scientists, graphs of a bit of human voice showing pitch on one axis, time on the other, and volume as the density of the resulting squiggle.

Unlike fingerprints, which are unvarying and are classifiable according to a system FBI tour guides can explain to Cub Scouts, voiceprints are as changeable as human speech itself, subject to factors such as head colds and intentional disguise and comparable only, as one voice analyst explains it, in terms of "gestalts," or highly subjective decisions about pattern recognition.

Looking back, it appears that the invention of the word "voiceprint," with its echo of the word "fingerprint," may have been Kersta's best idea. Indeed, the pop press seized on his dry bulletin in "Nature" and Kersta decided to go with the flow.

Soon, Kersta and Bell Labs parted by mutual agreement, and as he left he licensed the AT&T voiceprint patents, using them to establish himself as a manufacturer and salesman of "voiceprint machines." (Since the separation, Bell Labs has pursued the same line of work intensely, but in prudent silence.)

Kersta began performing such feats as using voiceprints to translate the garbled last call from an airliner which crashed at sea. (He said a maniac had shot the pilot, an hypothesis impossible to confirm or deny.) When a London newspaper gave him a tape supplied by Israel, Kersta verified that two voices plotting to blame the Six-day War on England and America were those of Nasser and Hussein.

By this time, some of Kersta's fellow speech scientists were pulling him aside to urge restraint. Others signed up for his course.

Graduates of the course, even those who later turned against the master, get misty and vague when questioned about the guts of it—the methodology of voiceprint identification. The exact technique remains as secret as a meditator's mantra, available nowhere in the public prints, which is odd, considering the growing number of voiceprint convicts languishing in cells.

At first, the courts didn't seem to mind this. Kersta's triumphs included his match of a black suspect's voice with that of a man who, back to the camera, had described his acts of looting and pillage in the Watts riots for a CBS documentary crew. (CBS had supplied the tape willingly.)

The reversal of that conviction got considerably less publicity than the trial itself, but the eventual result was Kersta's forced retirement as an expert witness. By 1968, voiceprinting as a forensic tool had become merely a nifty idea with insufficient lab data to prop it up in court.

This is where Ernie Nash comes in. He was working in the Michigan State Police Criminal Identification Unit, a fancy name for a fingerprint lab, and voiceprinting appealed to him as a cop with a good grounding in electronics.

Acting on his own, Nash went to the speech department of the local university, Michigan State, and talked about voiceprinting with Dr. Oscar Tosi, an Argentine speech scientist who felt Kersta's idea was sound, but needed more formal study.

Soon, Tosi and Nash were a team like Nero Wolfe and Archie Goodwin—that mixture of brains and legwork so appealing to mystery writers and readers. The Law Enforcement Assistance Administration blessed their union with half a million dollars.

This pleased the other speech scientists, some of whom had come to enjoy the bit of fame voiceprinting had brought to their musty corner

of scholarship. Tosi and Nash were going to plug up all the holes in Kersta's first, hurried studies, which had been performed with high school girls as his identification experts. Voiceprinting was going to be respectable.

Perhaps unsurprisingly, Tosi and Nash found their first test results so heartening that they were moved to begin assisting prosecutors with identifications and testimony—but before their results were printed in the scholarly journals. The upshot was a schism among speech scientists which continues to this day, and is getting worse.

When it comes to acoustical spectrography, "scientist" can mean anyone from a speech therapist to a mathematician interested in helping computers understand verbal commands. The only clearing-house which comes close to sheltering a consensus is a credentials-checking subcommittee on technical publication maintained by the Acoustical Society of America.

This committee is on the record with a unanimous condemnation of the use of acoustical spectrography in court, pending much further work, but the scientists involved in the action have gone to no trouble to call it to the attention of judges and juries. Some say frankly that such an action might spell an end to valuable federal grants.

Against such a day, which may be soon, Tosi and Nash have incorporated an International Association of Voice Identification, headed by themselves, to certify expert witnesses in the field. Certification takes three years, which leaves Tosi and Nash and their close associates firmly in control until 1975.

People such as Michigan state troopers and members of California's state intelligence unit seem to be progressing nicely by the IAVI's standards. A Ph. D. who signed on as an apprentice voiceprinter testified for the defense in a recent trial and found himself suddenly cut off from the association's steady stream of newsletters and training bulletins.

A watershed event happened in July, when Tosi and Nash appeared in San Rafael, a suburb of San Francisco, to testify against Stephen Chapter, 27, a phone company employee Nash had identified as the source of a recorded bomb threat against Mother Bell herself.

Pacific Bell's security office had asked Chapter and his colleagues to submit to recordings duplicating the bomb threat. All but Chapter agreed, and Chapter's voice was recorded without his knowledge and sent along to Nash with the others, but marked "employee who would not count."

Nash usually testifies that he needs 10 matching prints to make a positive identification. In the Chapter trial, several of Chapter's condemning "eights" turned out to be the letter "e," as proven by the work order Chapter had been reading when he was recorded without his knowledge. Confronted with this, Nash stuck by his identification.

Identical voiceprints from different people are more common than Tosi and Nash like to admit on the stand, and scientists helping with Chapter's defense had sought in vain for a matching voice for use in the trial. Luckily for Chapter, the prosecutor had sent Nash a blind tape of the defendant and six control speakers uttering the bomb threat. Working without labels such as "employee who would not count," Nash mistakenly matched the bomb threat with a voice which turned out to be that of the prosecutor trying the case.

Judge Warren McGuire's written opinion in the acquittal was a devastating, if courtly, attack on Tosi and Nash, but one which, due to the court's low station, is of little or no use beyond California's superior benches.

Chapter's jobless and denied unemployment compensation by the phone company's wrath, is suing Pacific Bell and the voiceprinters for $1.1 million in damages, and the Marin County district attorney recently announced he would defend Nash in that case at state expense.

Since the Chapter trial, Tosi and Nash have not been seen conversing together in courtroom or hallway, and the LEAA appears to have backed away from the idea of funding a permanent voiceprint institute for them at Michigan State.

Last month, in the bomb-threat case of a 22-year-old postal employe in Scranton, Nash materialized with a new scientific sidekick, Dr. John McClung of Wayne State University, a name utterly unknown to the ASA's little committee on technical communication.

That committee meets in Los Angeles this month, faced with a request from Bill Yurich, one of Chapter's defense lawyers, for permission to deliver a plea for firm action against what one scientist has called "Tosi-Nash Syndrome." Unless disqualified as an outsider, Yurich will be asked to stick to a written script cleared in advance by a committee of scientists, and the whole thing may be subject to what amounts to a continuance, so that Tosi and Nash can get a rebuttal together.

But even if the Acoustical Society remains dormant, ad hoc opposition to Nash is growing.

A noisy opponent is Dr. Louis Gerstman of CCNY, a psychologist specializing in speech perception. Appearing last month on a Canadian radio show about the Watergate tapes, Gerstman declared flatly, "voiceprints do not exist."

Gerstman and Nash collided in New Orleans last month at Jim Garrison's bribery trial. Nash testified that voiceprint analysis confirmed the integrity of the taped conversations the federal prosecutor sought to nail Garrison with. Gerstman testified that they were sloppy confections of many different conversations, and the jury believed Gerstman, acquitting Garrison.

In a New Bedford murder-kidnap case this month, Gerstman poohpooed Nash's match based on two whispered prints, pointing out that Nash had abandoned his personal standard of 10 matches, and that whispers provide too little data to work with. (Questioned on the stand in New Bedford about his performance in the Chapter case, Nash testified that he had been "misled" by the defense.)

Attorney Yurich and his boss, Bob Moran, were hired by Chapter's union, but many, if not most, voiceprint defendants to date have been poor people with court-assigned defense lawyers. Even if such lawyers find out about countering witnesses, they are faced with the costs of flying them in. Nash and his cohorts are flown in by prosecutors who may be thinking about buying one of the new "snub-nosed" police model voiceprint machines under LEAA assistance.

Defense lawyers in future trials will be luckier. A data bank about voiceprint prosecutions is being organized at Golden Gate University School of Law in San Francisco. The man behind it is Associate Professor Bernard L. Segal, an old law partner of, at one time or

another, both Sam Dash and Anthony Amsterdam, and, with Amsterdam, author of "The National Defense Manual," a weighty volume in a field of practice with relatively little literature.

"What really shocks me is the ease with which these fakirs—that's with an 'i'—toot up voiceprints with their horns, making claims other scientists are unable to replicate," Segal says. "It's a general reflection that in criminal cases, instead of being scrupulously careful about what we use, because lives and reputations are at stake, we're willing to let this shit in without meeting general standards and criteria for evidence."

Working only with personal funds, Segal and two young aides are assembling transcripts of all the voiceprint prosecutions they can uncover. A psychologist is helping them prepare a long questionnaire for the defense lawyers involved in such cases, in hopes of uncovering the tactical flaw which led to voiceprinting's uncritical acceptance.

"The real villain is society's heavy need for a better way to deal with crime," Segal says. "But if you're doing an LEAA contract, the government doesn't want you to tell them the police shouldn't use voiceprinting.

"There's no reason not to develop scientific methodology, but pseudoscience is something else. They're saying: 'I'm Mandrake the voiceprinter. Here's my button. Here's my switch. . . .'"

[From the Wall Street Journal, Mar. 18, 1974]

Modern Detection—Police Weapons Range From Electronic Cops to Glowing Bacteria

Gear and Ideas Borrowed From Space Technology, Industry and the Military

GRANDMOTHERLY BILLINGSGATE

(By G. Christian Hill)

Los Angeles.—A car had been burglarized, and detectives had almost nothing to go on—only that three men had been seen fleeing the scene in an "old tan-and-white station wagon." No make, model, year or license number was available. It was clearly a case for Patric, the new electronic gumshoe at the Los Angeles police department.

Patric (for "pattern recognition and information correlations") is a computer system that does much of what a detective does, but does it infinitely faster. It is jammed full of data on individual criminal records and descriptions, crime reports, field interrogations, stolen vehicles, outstanding warrants, even the modus operandi of known criminals. By instantly cross-referencing bits of information fed into it, Patric can quickly build up more and more information, finally coming up with likely human suspects.

In this case, Patric searched its files and found another vehicle crime in a different part of the city, also involving men fleeing in a tan-and-white vehicle—but this time witnesses had provided a partial license number. Using that number, Patric located field interrogation

reports showing the names of five men who had been stopped in similar cars. It searched its past arrest file and found that three of the five had been arrested for theft from an auto in a previous case. It turned over the names to detectives, who promptly investigated and then arrested the trio for the latest burglary.

Patric took 15 minutes to produce the suspects; a human detective probably would have written off the case as not worth the hours or probably days of sifting required, with the likelihood that suspects couldn't be located anyway. Even in cases where there is more information available, the computer can save hours and days of detective work.

A "RESOURCE EXPLOSION"

Patric is part of a new police technology that is greatly extending the range and efficiency of the cop on the beat. After years of slow and painful development, sophisticated hardware and techniques borrowed from private industry, space technology and the military are now hitting the streets in what Los Angeles Police Chief Ed Davis calls "an explosion in police resources." Increasing use of the new gear among the nation's 15,000 police agencies is already claimed to be curtailing crime rates and increasing arrests and convictions where offenses have been committed.

The gadgetry employed ranges from computers, helicopters and low-light cameras to such exotica as vials full of bacteria that glow in the presence of heroin, and explosives and "stress evaluators" that indicate whether a suspect is lying or not by measuring voice frequency. More new gear is still under development, including a miniature two-way radio.

Until recently the men in blue couldn't afford much new equipment. But now they're getting a big cash infusion from the federal government's Law Enforcement Assistance Administration (LEAA), an arm of the Justice Department. LEAA is pumping about $800 million a year into the various states, much of it going to their police organizations for equipment. Meanwhile LEAA's own equipment-systems-improvement program is aiding in the development of still more gear to be speeded to police in the field.

Deterring crime—as opposed to catching criminals when it's too late to undo the damage—is a major goal, and some of the new technology has been effective in doing just that. One key item: the low-light surveillance TV camera, which is sensitive enough to "see" even in semidarkness. In what is believed to be the first major use of extensive low-light TV surveillance, the city of Mt. Vernon, N.Y., installed two cameras at each end of its main business street in April 1971. Mt. Vernon publicized the installation widely. The result: a 60% drop in "observable" crimes, such as burglary, robbery, and assault.

PROMPT ARREST, PROMPT PURCHASE

Subsequently, Hoboken, N.J., began monitoring a high-crime section of that town with low-light cameras, and the crime rate plummeted. Mayor Steve Capillo now wants to extend the system widely. New York has begun scanning one of the city's major crime areas,

Times Square, and Detroit is now considering using it downtown, around its police stations.

Though principally used as a deterrent, the cameras can sometimes aid police in making arrests when a crime is in progress. A representative of Sylvania Corp. was demonstrating a low-light model to Cleveland police in a parking lot at night. The device happened to pick up a man breaking into a car; the police promptly arrested him and almost as promptly bought the system.

STALKING BY HELICOPTER

In one experimental program funded by LEAA, the Los Angeles County sheriff's department mounted low-light cameras with sound accessories in patrol cars on the drunk-driving beat. Drivers pinched on drunk-driving charges are shown sound tapes of their own behavior on arrest. Only 2.6% of the 1,150 arrested by the camera squad have bothered to go to trial, partly because the tapes are such damning witnesses; one shows a sweet, grandmotherly woman, just the type to sway a jury, screaming at officers in billingsgate that would stun a truck driver.

The Los Angeles County sheriff's department has also pioneered in the use of helicopter crime patrols. Many departments have long used copters for emergency and rescue work, and now many of the 300 or so police agencies already owning them have them hovering over high-crime areas, where they serve both as a deterrent and an effective way to catch crooks when a crime has been committed. When first employed in the Lakewood area of Los Angeles County in the early 1960s, they were credited with driving the crime rate in that area down 8% while elsewhere in the county it rose 9%.

In Los Angeles, copters now are used to follow cars suspected of making drug pickups at airports. They stalk robbery suspects to their homes, and corner fleeing suspects. Patrolling public facilities such as school grounds, where vandalism has lately become a major problem, they are credited with reducing the incidence of such mischief by as much as 70%.

Police say the helicopter sometimes panics criminals into surrendering when officers didn't realize they had done anything wrong. A helicopter crew in Los Angeles was recently hovering over a supermarket where a suspected check forger was trying to pass a bum draft. The crew was surprised to see two accomplices in a car get out and surrender to an accompanying ground patrol in the erroneous belief the copter crew had them spotted. Two other men in a getaway car recently gave themselves up during a bank robbery for the same reason. Officers actually didn't suspect they were involved in the crime.

Computer systems, including ones similar to Patric, are perhaps the most significant elements of technology now aiding police. One of their biggest contributions has been a vast improvement in communications, a perennial problem and a major one.

Ordinarily, in a noncomputerized police force, dispatchers at station houses are flooded with radio traffic from cruisers, crime reports from desk personnel and other messages. During peak crime hours

the dispatchers are frequently overwhelmed; in Kansas City, Mo., for example, police-radio voice frequencies get so clogged that officers in the field can't get through to the dispatcher 35% to 65% of the time.

Now many police forces, including Kansas City's, are installing computer terminals in patrol cars. Connected by their own radio frequencies to central computers (which in turn may have access to other computer memories at the state, regional or national level), the terminals allow patrolmen to bypass the harried dispatcher when they want certain kinds of information—for example, license numbers on hot cars and outstanding warrants or rap sheets on suspects picked up in the field. A cop in the car queries the computer, using a keyboard on the terminal and gets an answer in seconds. The system has already demonstrated that it can magnify many fold the policeman's ability to investigate and apprehend.

In Chicago, police report that two patrol cars carrying test terminals for a month recently made seven times as many "hits" on hot cars as they did without them. This was because they were able to make many more inquiries through the computer than any human dispatcher could handle. "The increase was so dramatic we didn't even keep track," says Sgt. Joseph Kalinowski of the department's research and development division.

CHECKING EVERYTHING IN SIGHT

The sheriff's department in Palm Beach, Fla., has been using in-car terminals for almost a year, and patrolmen are having a field day catching car thieves. "They just keep poking thousands of license numbers on everything in sight" into the computer to see if the sighted vehicles have been reported stolen, says Sheriff William Heidtman. "When it's quiet," he adds, "they go through motel and other parking lots." Since the terminals went in, stolen-car recoveries have climbed 60%.

Within a month or two, the New York police department will test the same system in 20 cars. Las Vegas has ordered units for 52 cars, and the Los Angeles police department plans to have 200 of its cars fitted within a year. The Los Angeles force also has an LEAA grant under which it is developing a new computer technique; under it, every police station in the city would eventually be wired into a central computer system that would automatically handle incoming calls, keep track of the location and status of all police vehicles, and deploy them in response to the calls.

Police are experimenting with any number of other gadgets with mixed success. One is the bioluminescent detector—essentially, a container full of bacteria that glow in the presence of a gaseous effluent given off by explosives and heroin. The New York police are using it now, though there are complaints that it sometimes glows when it shouldn't.

"SEEING" IN THE DARK

Police in a number of departments are also assessing infrared detection devices, which enable the user to "see" suspects in the dark by picking up their body heat. There appear to be a few bugs in such applications, however. Looking for a burglary suspect in an indus-

trial park, a night copter patrol of the Los Angeles County sheriff's department used an infrared detector to spot what it thought was the miscreant's heat emissions in a clump of bushes. The copter directed a ground patrol to the spot, where bluecoats closed in—on a warmly fermenting sack of manure.

Other items now under development appear to have promising futures. LEAA researchers working with a special fiber developed by Du Pont Co. say they will have a new lightweight ballistics shirt, capable of stopping a .45 slug at pointblank range, ready for testing this summer. They say they are about a year away from final development of a two-way radio, slightly larger than a cigaret pack, that employs space-and-solid-state miniaturization technology.

For every new item that gains acceptance in crime-fighting, however, many are discarded. In the past several years, manufacturers have rushed out all manner of gadgets, including riot tanks, ballistics shields, machines that spew forth foam, bubbles and slippery substances, and disabling crowd-control sprays (including one spectacularly messy variety that causes loss of control of the bowels and bladders). Most have never caught on.

A "slippery banana" machine, for example, throws a slick substance over an area and makes it impossible for a crowd to move over it. Alas, it is also impossible for police to move over it, and Chicago cops using it found it was nearly impossible to remove, too. "We had to peel it off the top of the asphalt to get rid of it," says Sgt. Howard Knight.

Ouch!

Thomas Crockett, research director for the International Association of Chiefs of Police, blames part of the high incidence of product unsuitability on the paint-it-blue syndrome. This is the tendency of some manufacturers who have developed an item for NASA or the military to just paint it blue and try to sell it to the cops, instead of taking the trouble to modify it to meet specific police needs. And, he adds, other manufacturers are rushing to market without adequate performance testing.

Mr. Crockett recalls one company that demonstrated its new bullet-proof shield by having a rifle fired at it as it stood before a building. "The slug went right through the thing like a hot knife through butter," he says. "We just stood around and gaped at each other."

Police agencies also gripe about the secretiveness of their principal equipment developer, the Pentagon, and its unwillingness to share some technology that the chiefs' association believes would be valuable.

Police covet the military's new super-quiet helicopters, for example, and they are interested in military gas masks that don't require awkward cannister attachments. But they have had little luck wringing information out of the government, despite pleas to LEAA and the Pentagon.

Mr. Crockett says the chiefs' association has gotten "a runaround" from government sources, who cite security classifications on some of the technology as the reason for not releasing it. "It's a tough street to work," says Mr. Crockett. "We lurk in the wings, trying to pick up information we're not supposed to have, so we can then build a case for getting it openly."

[From Computerworld, Apr. 10, 1974]

X-Ray Machine Probes Brain's Depths

New York.—A computer-controlled X-ray machine able to probe nooks of the brain previously unexplored by the medical world is "the most revolutionary breakthrough in X-ray technology in 50 years," according to Dr. John Evans, chief radiologist for the New York Hospital-Cornell Medical Center.

The machine, called an EMI-Scanner after the British firm EMI Ltd., is used to diagnose strokes, effects of "hardened arteries," hemorrhages, tumors and birth defects.

DISTINGUISHED DENSITIES

Its clinical worth, explained Evans, lies in its ability to differentiate brain tissue densities 100 times better than the conventional X-ray. Each particle of the brain absorbs a different amount of X-ray radiation when bombarded, and the X-ray machine is designed to perceive these differences and distinguish the individual tissues graphically.

But ordinary X-ray machines, he continued, only have the capability to pick up "major" differences, whereas the sensitivity of the EMI-Scanner allows "minute" differences to be readily detected.

The diagnostic test, which costs less than an ordinary brain X-ray because it requires no hospitalization, takes only four minutes and is painless, Evans said. The patient merely lies on an examining table connected to the scanner and sticks his head into the machine, which resembles a front-loading washing machine.

DOUBLE DATA

After 160 X-ray readings are taken, the information is processed by a Data General Nova 820 and is released in two forms. The first is a printout which shows tissue densities through a pattern of numbers, and the second is via pictures shown on a CRT screen where they are photographed for the permanent record.

Evans explained that by comparing pictures taken at different levels of the brain, it is possible, for example, to determine the precise depth of a tumor. With the conventional X-ray, the different levels of the brain are all superimposed in one picture. He also points out that the ordinary X-ray cannot show the slices of the brain in cross-section.

EMI said 50 hospitals around the world have placed orders for the system.

[From the Los Angeles Times, Apr. 11, 1974]

Following is a commentary on a story printed March 21 in View on the proposed Center for the Study and Reduction of Violence at UCLA. Dr. Ziferstein is associate clinical professor of psychiatry at the Neuropsychiatric Institute at UCLA and a life-fellow of the American Psychiatric Assn.

Critic of Violence Center Speaks Out

(By Isidore Ziferstein, M.D.)

Increasing public anxiety about violence and crime is reflected in the attitudes of public officials, who have put forth the proposition that the way to stop and prevent violence is by suppression and punishment.

Recently, these public officials have shown an interest in using new technological approaches for the purposes of mass screening, predicting, keeping under surveillance and actually controlling the behavior of "violence-prone" individuals and groups. A typical example is a proposal by Joseph Meyer of the National Security Agency to attach miniature tracking devices called transponders to arrestees and criminals as a condition of parole. The transponders would be linked by radio signals to centralized computers. Meyer suggests that eventually transponders could be used for "monitoring aliens and political subgroups" as well.

Unfortunately, this kind of thinking is now penetrating into the ranks of behavioral scientists. As funds for behavioral science research dry up, increasing funds are being made available for research on reduction, or prevention, of violence, using many new psychotechnologies.

ETHICAL IMPLICATIONS

One example is the work of Dr. Jose M. R. Delgado, formerly of the Yale University school of medicine, who devised techniques for inserting tiny electrodes deep into the brain. He stated that current research efforts "support the distasteful conclusion that motion, emotion and behavior can be directed by electrical forces, and that humans can be controlled, like robots, by push-buttons."

Many behavioral scientists have been deeply distressed by the ethical, legal and social implications of these new developments. This concern was heightened when it was learned that on Sept. 1, 1972, Dr. Louis Jolyon West, director of the Neuropsychiatric Institute at UCLA, formulated a proposal for a Center for the Prevention of Violence which would be financed with $1.5 million of federal and state moneys, in the first year and many more millions in subsequent years.

In this proposal, Dr. West states, "In some patients, outbursts of uncontrolled rage have definitely been linked to abnormal electrical activity in deeply buried areas of the brain. Techniques have recently been devised which may permit surgical treatment of violence-producing epileptic foci hitherto inaccessible."

Dr. West also states, "By implanting tiny electrodes deep within the brain, electrical activity can be followed in areas that cannot be measured from the surface of the scalp. It is even possible to record bioelectrical changes in the brains of freely moving subjects through the use of remote monitoring techniques. These methods now require elaborate preparation. They are not yet feasible for large-scale screening that might permit detection of violence-predisposing brain disorders prior to the occurrence of a violent episode. A major task of the center should be to devise such a test."

Proposals of this sort aroused grave suspicions and protests, among faculty, students and in the general community. As a result, there have been successive changes in the proposals. These included a succession of three different coordinators, five changes in the name of the center and a number of major revisions in the research proposals themselves.

First to be removed was any mention of "surgical treatment of violence-producing epileptic foci" and "implanting tiny electrodes deep within the brain." Also eliminated was the name of Dr. Frank R. Ervin, the coauthor of a book, "Violence and the Brain," which described "the production of small focal areas of destruction in parts of the limbic brain which will often eliminate dangerous behavior in assaultive or violent patients." (Dr. Ervin was listed as a researcher on two research projects in Dr. West's proposal of Sept. 1, 1972.)

By now, a serious credibility gap had developed, and many reputable behavioral scientists concluded that the successive changes in the proposals were in reality "launderings" in response to criticisms and protests. This credibility gap was widened when Dr. West maintained in an interview in the UCLA Daily Bruin of Jan. 25, 1974, that "human experimentation, psychosurgery, experimentation on prisoners" were never proposed. (It should be noted, in this connection, that in his proposal of Sept. 1, 1972, Dr. West stated, "New drugs now being tested in Europe and (very recently) in America, hold promise for diminishing violent outbursts without dulling other brain processes. These drugs should be tested in the laboratory and then in prisons, mental hospitals and special community facilities. Proper experiments must be done as soon as possible.")

DR. GOLDEN'S REMARKS

Dr. Joshua Golden's credibility is not enhanced when he says, "There has never been any intention of doing psychosurgery" and that "It was never intended that (Dr. Ervin) do research or be involved in the planning of the center, despite a New York Times report to that effect. The truth has been scrupulously ignored." (L.A. Times, March 21, 1974, View Section, Page 7)

Public apprehension was increased when it became known that Dr. West had proposed that some of the center's work be done at a Nike missile base in the Santa Monica mountains, saying, "It is accessible, but relatively remote. The site is securely fenced. Comparative studies could be carried out there, in an isolated, but convenient location, of experimental model programs, for the alteration of undesirable (sic) behavior."

Dr. West and Dr. Golden, the third and most recent coordinator-designate of the center, have attempted to minimize the opposition to the center by creating the impression that the critics are not scientists or mature citizens, but a "leftist opposition" comprised largely of students from the Progressive Labor Party and Students for a Democratic Society. (This impression is conveyed in the article by Ursula Vils, in the Times of March 21.) The opposition is also described by Dr. Golden as "cynical" and as "scrupulously" ignoring the truth.

EARLY STATEMENT

The truth which is ignored by Drs. West and Golden is that one of the early public statements of criticism of the proposed center was issued by the California Senate Committee on Health and Welfare after holding hearings at which Dr. West and other proponents and opponents were heard.

Other groups which have voiced criticism of the center include the Task Force on Alternatives to Violence, representing the Southern California Psychiatric Societies and the Assembly of California Branches of the American Psychiatric Assn.; the Northern California Psychiatric Society; the staff of the Research Operations Division of the Law Enforcement Assistance Administration of the U.S. Department of Justice; the American Civil Liberties Union of Southern California; the Children's Defense Fund of the Washington Research Project Inc.; and the Los Angeles chapter of the Federation of American Scientists, among others.

Senator Sam J. Ervin Jr., chairman of the U.S. Senate subcommittee on Constitutional Rights of the Committee on the Judiciary, inserted into the Congressional Record of Feb. 19, 1974, his year-long correspondence with the Law Enforcement Assistance Administration, in which he voices serious criticisms of the UCLA center.

[From The Washington Post, May 30, 1974]

Security Comes to Capitol Hill

MAIL AND VISITORS TO CONGRESS ARE NOW X-RAYED

(By George C. Wilson)

Mail to members of the House Judiciary Committee—the congressmen now weighing the impeachment evidence against President Nixon—is X-rayed for bombs these days.

Another X-ray device, with a television screen attached, looks through the attache cases of people entering one of the East Front doorways of the Capitol.

And a big pile of dirt—with a Vietnam-type bunker alongside it—is now in the front yard of the world's greatest deliberative body. The earthworks are part of a system designed to spot any prowlers who might sneak into the Capitol building at night—even if they went by sewer or water tunnel.

These are among the more visible pieces of evidence of tightening security at what was—until fairly recently—a free and easy atmosphere within the halls of Congress.

The bomb that went off March 1, 1971, on the Senate side of the Capitol is one of the big reasons for the changed atmosphere—even though no one was hurt in that explosion, five representatives were shot right on the House floor in 1954 by Puerto Rican extremists.

Another reason is the advent of the letter bomb. And a third is simply that protective sensor technology is available—thanks to some

extent to the Vietnam war, where the American military turned to industry for electronic gadgetry to offset the stealth of the guerrillas.

Capitol police officers and other people connected with the surveillance system being installed on Capitol Hill get edgy when asked about it, though its design was discussed openly in 1972 when Congress voted the money. (The cost, originally put at $3 million, is now estimated at $4.4 million.)

Police said the workers digging the big trench on the Senate side of the Capitol, for example, were not supposed to know they are laying the plastic pipe for the television cables that will connect the Capitol building with the two Senate buildings. But the project is becoming too visible to ignore.

George M. White, architect of the Capitol, said that he realizes the Capitol is "the people's building" and that any surveillance must be as unobtrusive as possible: "The whole principle has been to do as much as could be done and still retain an open building."

The X-ray machines looking through the mail of senators and representatives are not obtrusive to people visiting the Capitol because they do not see them. The machines work in the recesses of the separate Senate and House Post Offices.

In the Senate Post Office, all the mail is X-rayed. The House load, a million letters a month, is too much to put through the machine with the present staff. So the House postal executives pick out the mail most likely to be explosive—literally.

Right now, Watergate is considered the most explosive issue. Therefore, the House Post Office X-rays—500 at a time—letters addressed to the House Judiciary Committee and its individual members.

"Let's face it," said one congressional post office official. "There are a lot of sick people in the world. They have to be sick to send a letter bomb in the first place and then to think it would be opened by a congressman himself. It's always some secretary who opens it."

Besides Judiciary's mail, any House member's mail is X-rayed on request.

The machine has signaled some suspicious-looking contents, according to a House postal official, but nothing lethal.

Architect White said the same is true of the new X-ray machine looking now through packages carried into the Capitol through the document entrance on the House side of the East front. He said similar machines will go on duty at the rest of the entrances to Capitol Hill buildings "within weeks."

"The X-ray units are the safest that are known," said White about the radiation emitted. He said visitors have made no complaints so far about having their parcels X-rayed. The machine profiles any solid objects on a TV screened monitored by a Capitol policeman. At other doors, packages are opened by guards.

The big hole in the Capitol's front lawn is the only one that has to be dug for the security system, White said. It was made to punch through a passageway for the cables that connect TV cameras trained on dimly lit hallways all night long. The images are preserved for "instant replay" in case police want to use the film for evidence after an intruder is apprehended.

Yet another part of the security system being installed to protect lawmakers and the property on Capitol Hill is a hidden alarm, intended to go off if someone pries a locked window or tries to enter through an air shaft or sewer.

[From the Washington Star, Apr. 8, 1975]

Capitol Security: $4.3 Million

(By William Taaffe)

Four years after a bomb ripped through a section of the U.S. Capitol here, an elaborate security system that probably would have prevented the explosion is being installed. The cost to taxpayers: $4.3 million.

The system, a reaction to the 1971 bombing and other terrorist acts which have beset this country in recent years, is designed to provide lots of security but little inconvenience for visitors to the Capitol, most of whom will never know the extent to which they are under surveillance.

Since the bombing of the Capitol, guards generally have limited their security efforts to inspecting briefcases and barring tourists after certain hours. But by May 1, when the new system is completely phased in, protection of the building will become highly sophisticated.

On that date, 108 television cameras in the Capitol and the five House and Senate office buildings will begin monitoring certain hallways round the clock. Police, in a special command center, will be able to push a button and obtain an "instant replay," as though they were watching a football game.

Most of the cameras have been installed, but it takes a few minutes to spot them. Visitors should look for a little black eye in a wall at the end of any well-traveled hallway. The camera, encased in metal, is hidden behind the wall.

Capitol officials last year began operating a second aspect of the security system—X-ray scanning devices similar to those in some airports—at main entrances to the House and Senate buildings.

Shortly after the impeachment hearings last summer, police at the Rayburn House Office Building set up the first X-ray machine which can detect anything from paper clips to automatic pistols in a visitor's briefcase. Guards look for outlines of suspicious objects on a video screen wired into the scanner.

Elliott Carroll, administrative aide to Capitol architect George M. White, said the eight scanners now being used on the Hill are still in a "shakedown" stage but will provide significantly more security with little inconvenience to visitors when working perfectly.

The need for privacy evidently was a consideration in the $270,000 expense for the X-ray machines. White told a House subcommittee that approved the outlay that open inspection of parcels has caused "embarrassment and consternation" among visitors and employes.

The final part of the surveillance network might even thwart Agent 007 if he tried to pierce security by hiding in an air-conditioning duct

or infiltrating through the 3½ miles of heating and water tunnels beneath the Capitol.

Electronic detection devices, already in use primarily at night and in areas where the television cameras don't reach, pick up any movement and register an alarm in the 24-hour control center. The range of the devices appears to be unusually broad.

"If somebody picks up a manhole in the street and attempts to penetrate the system, (the devices) will record or sound an alarm" in the control area, located in a vacant section of the original trolley tunnel between the Capitol and the Russell Office Building, White told the subcommittee.

The combination of strategically placed cameras and motion detectors will give police leverage in isolating a potential bomber: Once an alarm sounds indicating that someone has broken into the Capitol, the cameras can chart his progress until officers arrive.

The instant replay will serve two purposes, authorities say. It will allow guards to examine suspicious movements in slow motion within three seconds and if the interloper is captured, the tape can later be used as evidence against him. The video operation cost more than $1.8 million.

Capitol officials are reluctant to discuss details of the new system, but it appears to offer security similar to that at the White House, where, White said, the same equipment is being used "unnoticed and undetected by the millions who visit there each year."

For all its benefits, the system isn't foolproof. A member of the Secret Service who worked on the plan told lawmakers, for example, that the X-ray machines would detect a time bomb but probably would fail to discover an explosive that detonates when a parcel is opened.

In addition, there are 90 entrances to the various Capitol buildings, and although guards control access at each of them, manual inspections of packages are only as good as the men who do the checking.

The new system, however, probably would have prevented Puerto Rican nationalists from shooting five congressmen on the House floor in 1954 and stopped the bombing. And that, officials say, would have made the system useful.

[From the Manchester Guardian, June 4, 1974]

(Simon Winchester on the lie detector world of Big Brother and Dan Dare)

Spotting the Truth in a Bead of Sweat

This week 12 congressmen sitting on an obscure House subcommittee have been hearing a tale that makes Dan Dare sound like medieval melodrama. They were told about a device now supposedly being tested in Israel, on a slight hill overlooking the Allenby Bridge, which can tell from half a mile whether a man—and in this case the man is nearly always an Arab—is telling the truth or not.

The machine is known as a "microwave respiration monitor," and the men who operate it are members of the Israeli police force. According to testimony given in Congress by lawyers, with the American

Civil Liberties Union, the policemen on the desert rise aim their device squarely at the solar plexus of any Arab trying to walk across the river bridge. Soldiers at the crossing point question the would-be immigrant: the microwave signal playing on his stomach tells the distant policemen if he is breathing more rapidly under the questioning than is deemed normal. If he is, the policemen radio down to the bridge that they suspect the man of telling lies; and without further ceremony, the luckless Arab is brusquely turned away.

The device, say the ACLU "offers the possibility of widespread, random, remote, and surreptitious 'truth verification' at border crossings, airports, police line-ups, perhaps even Congressional hearings." Would that John Dean had known that.

The Israeli device, under development, according to the ACLU at the Weizmann Institute there, is only one of a darkly threatening battery of new devices that belong to the burgeoning crop of "crime fighting machines." Another is the truth verification mould being developed now in the laboratories at Kent State University in Ohio, an institution that might be thought to have a perfectly understandable fear of the crime fighting establishment.

The Kent State machine claims to be able to tell if a man is lying even if he doesn't open his mouth—if he so much as thinks a falsehood, that is apparently enough. It works by measuring the response to questions and comments of the human eye: it calibrates, enormously accurately, minute and momentary changes in the size of the pupil, retina, and the eye's overall focus. It can tell if a drugged or drunk person is being truthful: it can probe behind the Fifth Amendment; it can drag a comment from a "no comment"; already men applying for jobs on the campus police force have been screened with the device, and so far, such is the state of what has been called the "security mania" currently sweeping America, no one has tried to put a halt to the procedure.

The development of the lie detection industry has come under attack recently because of an increasing practice among employers to use polygraphs—as they are now popularly called—against potential employees. Often these days applicants are warned that a failure to subject oneself to polygraph test will almost certainly be a bar to getting the job.

One department store in Cleveland takes the use of the detectors even further. In the event of a shortage in a till, a warning note says on an employee's contract, "I agree to take a polygraph test administered by the Truth Verification Agency regularly engaged by the company. If I refuse to take the test I agree that the company may apply against the shortage any moneys otherwise due to me."

In other words take the lie test, or have your wages cut to make up the loss in the till.

But lie detectors are just a small facet of the vast crime warfare industry. Many of the other products of this growing monster were on display in mid April at the eighth annual Crime Countermeasures Conference held at the University of Kentucky, which maintains an interest in the field. Delegates came from every branch of the people-watching establishment; the CIA, the Secret Service, the Atomic Energy Commission, the FBI, with the Pentagon's Advanced Research Project Agency, and the army's Land Warfare Laboratory.

There were Britons there too: a Mr. Brian Hall of the Ministry of Defence; A. N. Rapsey of the Police Scientific Development Branch in St. Albans; J. E. Simes of the Scientific Advisory Branch of the Home Office; R. J. Drewett of Plessey Radar Research; Stanley Shorrock of a Blackburn research firm. Together with delegates from South Africa and Jamaica and Germany and Canada, Mr. Hall and his friends discussed such conceits as electronic cadaver detectors, laser sensors (Mr. Shorrock presented a paper on "Perimeter Intruder Detection System of Microwave Energy"), night vision devices, automatic vehicle monitoring systems and, perhaps most minatory of all, a vast range of machinery coming under the title of "personal identity verification system," whose development is masterminded by the Electronic Systems Division of the US Air Force.

One such machine now in production—and, like so many similar systems, first produced by the military under defense contracts, and now funnelled over for use against civilians—is the fingerscan Automatic Fingerprint Recognition System, developed by a Buffalo firm called Calspan Technology Products, Inc. "For truly reliably personal identification use an indisputable unchangeable non-transferable characteristic of the person himself—his fingerprints," says the brochure.

At a "lower per-portal cost than guards the machine is a box into which an aspirant entrant puts his hand. A light scans his fingerprints, transmits a mathematical version of his print to a central storage computer—which may be many miles away even in another city—compares it with prints from a central bank (the FBI has 190,000,000 in stock, only 10 per cent of which belong to criminals and then decides whether or not to open the door. If it says no, there is apparently no appeal.

The parallels with Orwell are too obvious yet, as organisations like Civil Liberties Unions are keenly pointing out, both here and across the Atlantic, no one in these huge television drugged societies seems to care or to mind very much. The famous cartoon of the family looking through a door marked "Police State seems all the more appropriate now. "My," says the woman peering through the crack, "it looks peaceful and safe in there."

[From The Washington Post, Aug. 25, 1974]

A.T. & T. Monitors Some Phone Calls

(By Ronald Kessler)

The American Telephone & Telegraph Co. is using a new device that permits its employees to monitor certain telephone calls by dialing a secret code from any telephone equipped with touch-tone dialing.

AT&T officials in New York said the device, which costs $1,200 and is known locally as the "silver box," is used only for monitoring calls made by customers to telephone company business offices.

The purpose, they said, is to determine how customer representatives are handling requests for new telephone service or billing corrections.

The procedure is necessary, they added, if the company is to maintain high quality service.

The officials said the device is not used for monitoring calls between customers.

The "silver box" monitoring system is part of a longstanding AT&T program of randomly listening to parts of calls between customers and between customers and business offices to determine quality of service. When listening to calls between customers, company employees—called service observers—are instructed to stop monitoring when conversation begins.

AT&T has said the program protects customer privacy at least in part because the service observers are selected for honesty and integrity. Under the old monitoring system, outsiders could not listen to calls—unless they installed a wiretap—because the calls traveled over telephone company wires.

The new system allows anyone with knowledge of a dialing code to listen in from any touch-tone telephone in the country.

The officials asserted the system is "secure" because the codes that permit access to calls are difficult to obtain and use. They said few employees know the codes, and any employee who disclosed them would be dismissed. The codes are changed periodically, they said.

However, this reporter obtained one code.

During the calls that are monitored, customers, who identify themselves by name and telephone number, discuss such matters as the dates when they plan to move, the hours of the day when they are normally away from home, the nature of their jobs or businesses, and the state of their finances.

C&P customer representatives interviewed by The Washington Post said an eavesdropper could also overhear records of long distance calls that are discussed when customers call to complain about bills. The representatives said it is not unusual for these records to list calls from the homes or offices of senators, congressmen, and other prominent persons.

At least three congressional committees are probing various aspects of AT&T's practices and policies concerning the privacy of customer calls and records.

The investigations stem in part from disclosures of the company's role in assisting the FBI to conduct wiretapping for national security purposes and in making available records of long distance calls to government agencies.

When the system was described to Fred W. Langbein, news service manager of C&P Telephone here, he expressed disbelief, "I don't see how you could live with that," he said.

William P. Mullane, AT&T director of public relations and employee relations, said, "Sounds unbelievable to me."

Langbein said he could find no one at C&P who was aware of the existence of the new system. He said the company's security officials were "dumbfounded" when they heard about it.

However, Paul D. Loser, AT&T's assistant vice president for customer assistance, acknowledged the system is in "underspread" use by 13 of the giant utility's 20 operating companies—including C&P.

Loser said the old system required the telephone company to link monitoring rooms by wire with company offices over a wide area. This

was costly, he said, and monitoring rooms in remote areas were manned by only one or two observers, who had no supervisors.

With the new system, Loser said, wiring to individual offices is not necessary, and monitoring for an entire state can be consolidated in one location. He said this improves security because all observers are supervised.

"It's more secure and less expensive if you can observe from a central location," he said.

Loser estimated that about half the listening devices used by AT&T can be operated only with a special touch-tone telephone not normally supplied to customers. More of the devices are being converted to this more secure system, he said. "Now that we are aware that one person could get in (to the system), we will accelerate the program," he said.

Charles L. Anderson, president of Tel-Tone Corp., a private, Seattle company that makes the listening devices, said the Bell System began buying them about three years ago. It has bought some 1,400 so far, he said.

Anderson said each listening device, about the size of a large cigar box, can monitor 10 lines and has a list price of $1,200. He said he sells the devices only to telephone companies.

The devices are installed in switching equipment behind service observation monitoring rooms. Each box is assigned a different, seven-digit telephone number.

To monitor calls, a listener dials the seven-digit number assigned to each box. When he hears a tone, he dials two additional digits in rapid succession. The tone lasts for two seconds, and if the additional numbers are not dialed while it sounds, the device disconnects.

Once the codes are dialed in proper sequence, the listener hears conversations on any one of the 10 lines connected to the device. By pressing another digit, the listener can successively switch to each of the other lines and hear different conversations.

[From Playboy Magazine, Sept. 1974]

Bringing the War Home

(By David M. Rorvik)

We got out of Vietnam, right? So the cops are using sensors that were field-tested on the Ho Chi Minh Trail and surveillance devices they can plant in your brain. Now, if they could just call an air strike at Park and 56th. . . .

From the first "peace scare" on, there was corporate, military and bureaucratic breast-beating and brain-trusting over the question: What will we do when the war in Vietnam is over? The enterprising answer that finally emerged: *Bring it home.* As early as 1967, Paul Baran of the Rand Corporation, the California think tank that attempts—successfully at times—to make prophecy a science, envisioned the use of exotic surveillance technologies on the domestic law-and-order front. He worried that "by moving in this direction, we could easily end up with the most effective, oppressive police state ever

created"; observed that "any new device created solely with a legitimate police activity in mind can and will probably be misused"; cautioned that the "new technologists must be men of high ethics"; and then went on to concede that high ethics have "never been regarded by my technical colleagues as a necessary prerequisite for those in the trade." He predicted that ways would be found to rationalize the development of domestic surveillance devices and, indeed, finally came to the rationalized conclusion himself that "the high payoff possible by investing more in technological development is so great that it would be shortsighted to outlaw the development of many of these new devices."

Government and industry obviously agreed. By 1969, the newly established Law Enforcement Assistance Administration (LEAA) of the Department of Justice had $63,000,000 to help local police Americanize some of the war technology and, in general, to develop more sophisticated weapons for the "war on crime." By 1971, the LEAA budget had rocketed to $480,000,000 and today is somewhere close to the one-billion-dollar mark. The House Subcommittee on Legal and Monetary Affairs, in a report critical of the new organization, noted that "no Federal grant-in-aid program has ever received a more rapid increase in appropriated funds than LEAA."

Ways were soon found to help Government, business and academic communities share this new fortune. Among other things, LEAA is pumping millions of dollars into new police-science programs—reminiscent of the now largely defunct R.O.T.C.—at universities across the land. And at a Carnahan Conference on Electronic Crime Countermeasures, a symposium that is conducted each year at the University of Kentucky for a number of law-and-order interests, Howard E. Trent, at the time Kentucky's assistant attorney general, told attending corporate engineers and law-enforcement personnel that "there is a great unrestricted area of electronic surveillance and electronic countercrime measures in which there needs to be expansion and further innovation." Stressing that legal restrictions on surveillance are few, he rallied the assembled with the intelligence that "the challenge is wide open."

By 1972, according to the Electronics Industries Association, U.S. corporations were accepting the challenge to the tune of $400,000,000. Their production of surveillance devices, "command-and-control" systems and police communications equipment under LEAA and other Government-agency grants was described by *Electronics* magazine as "part of a Nixon Administration shifting of resources from the Defense Department into domestic programs." Robert Barkan, an electronics engineer, writing in *New Scientist*, summed up the situation more directly: "American companies, faced with dwindling Federal funds for aerospace and defense, are eagerly looking for new markets. Surveillance equipment for the home front is a particularly easy transfer of Vietnam technology. . . . To industry, the choice is clear. The extent of its concern for the way technology can best serve humanity was succinctly expressed a few years ago by a vice-president of the giant Avco Corporation: 'We have a modest amount of altruism and a lot of interest in profits.'" Martin Danziger, asked while he was serving as assistant administrator of LEAA whether a number of

Buck Rogers-type weapons now being developed for control of domestic criminals, rioters and "dissidents" were really necessary, replied, "The business community has taken substantial interest in them, and I have faith in their judgment." Former Attorney General Ramsey Clark, under whom an embryonic LEAA was formed, warned that the organization "could be a disaster . . . funds that aren't specifically set aside for riot control could end up being spent to stockpile arms for use during riots or demonstrations. It's another potential, and an enormous one, for repression."

There is evidence that this potential is already being realized. Law and order has become big business. The Chicago police have an annual budget of nearly $100,000,000, the New York City police have more than $350,000,000—both big enough to qualify for *Fortune's* list of the 500 largest corporations. Some 40,000 police agencies, employing nearly half a million people, are clamoring for a bigger piece of the rapidly expanding action. And they're getting it. *Congressional Quarterly* reports that even some lowly backwash police departments, far from the front lines of Harlem and Watts, are getting equipment, including helicopters and tanklike vehicles, sufficient to quell small armies. One small community in Ohio, for example, recently acquired $230,000 worth of patrol cars, guns, gas masks and assorted other riot-control equipment, even though there has never been any hint of a disturbance in that area. Similarly, a small cow town in Montana got enough Mace to stop a giant stampede.

As the war technology is Americanized, the demand for ever more exotic surveillance and riot-control equipment is being answered. Start with our 3.25-billion-dollar "computerized battlefield," a complex of sensors strung along the Ho Chi Minh trail. Task Force Alpha, as it was called, was largely a failure, frequently mistaking wandering water buffalo for truck convoys. After bombing the hell out of animals, winds wafting through the buffalo grass and even raindrops—all of which activated the sensors—the Defense Department unplugged its rampaging white elephant and brought it home. Now the Justice Department's Border Patrol is trying to put it to more effective use detecting drug smugglers along the Mexican-American border. Remote-controlled pilotless aircraft developed for use in Vietnam may also be used to monitor the sensors and relay data to computer centers. There has been some Congressional opposition, but Sylvania Electronics Systems, which proposed the project, has sought to calm the uneasy in Government with the statement (contained in a "proprietary" report) that "the political implications of using surveillance equipment along a friendly foreign border have been considered by selecting equipment that can be deployed without attracting attention and easily concealed."

Other devices developed for use against the Viet Cong have been declassified and diverted to the home front. Among them are black boxes that can "see" through walls and low-light television systems that can spot a man in extreme darkness half a mile or more away. The black boxes—foliage-penetration radar developed by the Army to ferret out guerrillas in thick Vietnam jungles—are now being modified to penetrate brick and cinder-block walls. They are said to be useful in controlling civil disturbances.

Night-vision devices, employing recently declassified war components, are selling briskly to police. The devices can be mounted on guns, police cars, helicopters and building tops, then linked to closed-circuit TV systems that scan entire city blocks. The Singer Company, which manufactures some of the light-intensifying devices, notes that they have been effectively used "to monitor suspicious group meetings." In a number of cities, including San Jose, California, Hoboken, New Jersey, and Mt. Vernon, New York, police have set up hidden 24-hour surveillance systems to watch city streets. Despite citizen opposition to the Peeping Tom cameras, some of which are capable of penetrating apartment windows, a Government advisory committee has recommended that several million dollars be spent to establish a pilot 24-hour TV surveillance system covering nearly *60 miles* of Brooklyn streets, giving those monitoring the cameras (at a modest two dollars per hour) the fringe benefit of being able to zoom in on everything from a first-class mugging to a teenage petting session beneath the once protective shadow of an elm tree.

In another 24-hour surveillance system funded by the Justice Department, the state of Delaware was given a number of civilian trucks that, according to the grant, "are to be used as the basis on which patrol is to be conducted under covert conditions; e.g., uniforms of dry cleaners, salesmen, public utilities, etc., make it possible to be in a neighborhood without being obvious." The equipment was designed for covert photography "of persons whose activities are suspicious in nature."

Beyond those devices whose roots can be traced directly to the war in Vietnam, a perusal of some of the recent "Proceedings" of the Carnahan Conferences reveal the development of a wide array of new law-and-order gadgetry, either proposed or in the making, including "crime-predicting" computers; electronic license-plate scanners; national computerized fingerprint analyzers and data banks linked to orbiting police satellites that instantaneously relay information on individuals; postal X-ray machines that peep into letters and packages without breaking seals; bioluminescent bacteria that light up if you're stoned; hidden lie-detector machines that measure stress in your voice; "hand-held" dogs that are carried through crowds to sniff out drugs and explosives; hidden magnetic detectors and "low-dosage" X-ray machines that examine your body without your knowledge.

Other documents, such as a report entitled "Communication for Social Needs," prepared for former Presidential assistant John D. Ehrlichman, reveal that the Nixon Administration concocted a plan that would require the installation of FM receivers in every boat, automobile, radio and television set, thereby enabling the Government to propagandize day and night if desired. (Another Nixon proposal called for devices that could automatically turn radio and television sets on and tune them to "emergency" messages.) When the FM plan was exposed by Representative William S. Moorhead, chairman of the House Subcommittee on Government Information, Dr. Edward E. David, Jr., director of the White House Office of Science and Technology, denied that there was any intention of actually implementing the plan. Representative Moorhead remains skeptical, calling the plan a "blueprint for the Big Brother propaganda and spy system which

George Orwell warned about in his novel *1984*. The fact that the Government has been testing a system that would give it access to private homes raises serious questions about the truthfulness of Dr. David's statement."

But Big Brother must come equipped with more than just exotic ears. To be truly effective, he must also be able to deliver swift and persuasive punishment to those who stray too far or dissent too vigorously. Hence the emergence of a dazzling night gallery of "nonlethal weapons": the "photic driver," which delivers a toxic combination of light and sound pulses, inducing in the uncooperative epilepticlike "flicker fits" (giddiness, nausea, fainting and even convulsions); the Shok Baton, an electronic prod; the Stun-Gun, which fires pellet-filled canvas bags capable of knocking a man down at a range of up to 300 feet; "limited-lethality riot projectiles," such as 12-gauge shotgun shells filled with plastic pellets; plastic bubbles that immobilize rioters; indelible dyes to mark dissidents and make them easier to apprehend once crowds have been dispersed; darts loaded with immobilizing drugs; the "banana peel," a chemical that makes the ground so slick that one can neither walk nor drive on it; the "cold-brine projector," which slaps the dissident in the face with an incapacitating blast of icy liquid; the "instant cocoon," which sprays crowds with an adhesive substance that actually makes individuals stick together; and the "taser," a gun that fires electrified barbs that paralyze the victim.

Malignant as some of these command-and-control systems sound (and they are the same that LEAA endorses owing to the fact that "the business community has taken substantial interest in them"), they are not even remotely as diabolical as Big Brother's subtler weapons—the electronic "conditioners" that seek to *change* as well as deter the dissident. One of the most alarming proposals in the realm of behavioral engineering is that of Joseph Meyer, a computer expert in the supersecret National Security Agency. Writing in the *IEEE Transactions on Aerospace and Electronic Systems*, Meyer explains in exhaustive detail a system in which 25,000,000 Americans would be forced to wear miniature tracking devices ("transponders") linked by radio signals to centralized computers. "Attaching transponders to arrestees and criminals," he says, "will put them into an electronic-surveillance system that will make it very difficult for them to commit crimes, or even to violate territorial or curfew restrictions, without immediate apprehension."

It would be a felony, under his plan, to remove the transponders and, in any event, it couldn't be done without the computer's knowledge. The devices would be attached as a condition of parole or bail, but Meyer sees them being used for "monitoring aliens and political subgroups" as well. Heaping insult on injury, he proposes to pay for the system by leasing the devices to the "subscribers"; i.e., those who are obliged to wear them, "at a low cost, say five dollars per week." Thus, he declares, is *poetic* justice achieved.

Meyer, however, is not without heart. He observes that the criminal poor and other minorities are at a disadvantage in learning how to "get along" in our generally affluent society. He concedes that these minorities need more than "a long apprenticeship" learning to fit in. And that's where his transponders come in. They can provide the de-

prived, he says, with "a kind of externalized conscience—an electronic substitute for the social conditioning, group pressures and inner motivations" that keep most of us in line. For these people, he declares, an externalized conscience is as necessary as "a heart pacer [is] to a cardiac patient."

Even less is left to chance in a plan outlined by self-described "social gadgeteer" Ralph Schwitzgebel, Harvard psychologist and pioneering behavioral engineer. In a monograph published under a National Institute of Mental Health (Center for Studies of Crime and Delinquency) contract, Schwitzgebel describes a plan that would literally bug the body. It involves attaching and *implanting* miniaturized radio transmitters on and inside the bodies and brains of subjects in need of "rehabilitation," not only to monitor their conversations, locations and even sexual responses but to deliver electrical shocks whenever needed to counter undesired speech, behavior or physiological responses. Schwitzgebel dwells at length on the problem of "sex offenders," particularly homosexuals, noting that there are now devices available that can detect even the most minute penile changes. In the event of an "inappropriate" erection, the programmer—computer or human—can zap the offender with corrective kilovolts (at low amperage) and thus, over a period of time, effect a "cure." Schwitzgebel says he recognizes, as a lawyer as well as a psychologist, the threat such a plan poses to individual civil liberties but then proceeds to suggest ways in which the system could be implemented without provoking a constitutional crisis. In the meantime, he's holding a patent on a nonremovable wrist transmitter of his own design.

Perhaps the most terrifying part of the Schwitzgebel scenario involves the brave new world of E.S.B.—electronic stimulation of the brain. Human subjects have already been wired with implanted brain electrodes. The result is that human programmers can electronically order some of their subjects' actions and emotions simply by pulsing radio signals into specific parts of their brains at the desired moments. Dr. José M. R. Delgado, until recently of the Yale School of Medicine, a leading E.S.B. researcher, notes that lab animals "with implanted electrodes have been made to perform a variety of responses with predictable reliability as if they were electronic toys under human control."

Dr. Barton L. Ingraham of the School of Criminology at the University of California at Berkeley suggests that bugging the brain could provide not only continuous surveillance of those with "criminal tendencies" but also "automatic deterrence or 'blocking' of the criminal activity by electronic stimulation of the brain prior to the commission of the act." Dr. Ingraham concedes that the use of E.S.B. would "require a Government with virtually total powers" but sees a number of things in its favor, including the fact that it would be "completely effective" and "relatively cheap." As for the economy of the matter, an electrical engineer named Curtiss Schafer agrees: "The once-human being thus controlled would be the cheapest of machines to create and operate."

So far, the new behavioral engineers and "psychotechnologists" have confined themselves to the prisons, which many of them obviously regard as convenient laboratories in which they can utilize human

subjects whose civil liberties are not only dimly defined by society but poorly understood by the subjects themselves. At a 1962 symposium of social scientists and correctional administrators, James V. Bennett, then director of the U.S. Bureau of Prisons, was already urging the assembled to take advantage of the "tremendous opportunity" afforded by the 24,000 men then in the Federal prison system—"to carry on some of the experimenting to which the various panelists have alluded. . . . We here in Washington are anxious to have you undertake some of these things; do things perhaps on your own—undertake a little experiment of what you can do with the Muslims, what you can do with some of the sociopath individuals."

Among the things "alluded" to at that symposium were brainwashing techniques perfected by the North Koreans and biochemical restraints. By the late Sixties, some penal staffs included "prison thought-reform teams" that subjected the troublesome inmate to intensive group pressures, ridicule and humiliation in an effort to help him be "reborn" as "winner in the game of life." Drugs, aversion therapies that utilize pain and anxiety, sensory deprivation in which the subject is isolated from all or most stimuli, planned stress and psychosurgery might all come into play in the course of winning a new convert. Candidates for these elaborate therapies are often characterized in penal reports as uncooperative and revolutionary.

Jessica Mitford, in her book *Kind & Usual Punishment*, tells of a Maximum Psychiatric Diagnostic Unit (M.P.D.U.) for 84 convicts selected from various California penal units to serve as research subjects. Most, she observes, were chosen for having shown "disrespect for authority" or "because they are suspected of harboring subversive beliefs." (Thus, the Soviet tendency of equating dissidence with insanity, of the sort that might even justify radical psychosurgery, shows signs of proving equally useful in the "free world," or at least its prisons.)

Just what the M.P.D.U. 84 could expect was suggested at an assembly of behavioral engineers at the University of California at Davis in 1971. "We need to dope up many of these men in order to calm them down to the point that they are accessible to treatment," one suggested. "We also need to find out how he thinks *covertly* and to change how he thinks," said another. "Those who can't be controlled by drugs are candidates for the implantation of subcortical electrodes." One psychotechnologist calculated that at least ten percent of the men would "benefit" from psychosurgery designed to burn out the "source of aggressive behavior."

The courts have recently intervened to halt, temporarily, at least, some prison psychosurgery, concluding that prisoners are incapable of bona fide voluntary consent. Public outcry in other quarters has persuaded LEAA to withdraw the support it was previously giving several psychosurgeons. The psychotechnologists, however, continue to do battle. Dr. Ingraham is busy trying to persuade the authorities that the potential abuses of brain implants have been much exaggerated. In a recent Department of Justice monograph, he writes, "The new liberalism is . . . fanatical on the issue of extending legal due process into areas which were once considered reserved for the exercise of knowledgeable administrative discretion." Dr. Delgado, mean-

while, has removed his research to Spain for the time being. And in California, Ronald Reagan's proposed Center for the Study of Violence, previously shot down by fears that it would engage in improper experimentation, has been restored under a new name.

Finally, *World Medicine*, in 1973, six years after Paul Baran's prophetic Rand report, revealed that Rand was carrying out "exhaustive studies of 2000 cases of torture in South Vietnam to assess the viability of the methods used by U.S. forces." Could even this ugly part of the war be coming home?

Has 1984 arrived—ten years premature and crackling with teratological technologies that make Orwell's world look inefficiently quaint by comparison? The transponder generation has so far only been conceived, not yet hatched, and E.S.B. is still only a few barbs in a few brains. But upper-case Law and Order continues to grow, at the expense of personal liberty and privacy, and to grow by great leaps and bounds, involving not only the police and industry but even the military, which, with time on its hands, is looking for (and *finding*) a new enemy at home.

The Senate Subcommittee on Constitutional Rights recently revealed that the Armed Forces have been compiling massive computerized data banks on civilians, many of whom have never even been arrested. The military regards those on its lists not as "loyal Americans exercising constitutional rights but [as] 'dissident forces' that 'billet' and 'assemble,' carry 'weapons' and 'explosives,' contain 'an organized sniper element' and coordinate their assaults on 'targets and objectives' with 'communications equipment.' Civil-disturbance operations thus will be similar to counterinsurgency warfare (or counterinsurgency war games), in which military units will be the 'friendly forces' and demonstrators the 'opposing forces.'" The men in the domestic war rooms, the subcommittee found, "kept records not unlike those maintained by their counterparts in the computerized war rooms in Saigon."

The subcommittee reported that Army intelligence alone had "reasonably current files on the political activities of at least 100,000 civilians unaffiliated with the Armed Forces," and could draw upon an additional "25,000,000 index cards representing files on individuals and 760,000 cards representing files on organizations and incidents" compiled by other Government agencies. Much of the information contained in the military files, including financial, psychiatric and sexual data, the subcommittee discovered, had been gathered by covert means. "Convicted spies joined Nobel Prize winners and entries from *Who's Who* in the files," the report states, adding that the files pose "a clear and present danger to the privacy and freedom of thousands of American citizens—citizens whose only 'offense' was to stand on their hind legs and exercise rights they thought the Constitution guaranteed them."

The Young Democrats, the Liberal Party of New York, the League of Women Voters of the U.S.A. and even the Peace Corps were indiscriminately lumped in the files with the Communist Party of China and the Hell's Angels of California. Those listed as subversive included the NAACP, the American Friends Service Committee and a number of Congressmen and governors. "Short notations," the sub-

committee reported, "commented on the individual's political beliefs, actions or associations. For example, one person had 'numerous pro-Communist associates.' Another, a young black male with no arrest record, was described as an 'extremely radical, militant individual.' Other characterizations were . . . 'one of the most active Communists in the Cincinnati area' . . . 'reported to be a psycho' . . . 'wants to abolish the House Un-American Activities Committee,' 'paranoid trends' . . . 'participant, anti-Vietnam war demonstrations' . . . 'has Red background.' " One nationally known civil-rights leader was said to be "a sex pervert" and was "known to have many known affiliations." One individual was damned for having been "active in the state of Texas" (no further information), another for "failure to comply with a school policy involving female students."

The absurdity of all this is summed up in the following "intelligence" report, which would be funny were it not delivered in such deadly (and costly) earnest: "A. First The Crazies [an offshoot of the Youth International Party, better known as the Yippies] plan to enter Bellevue Hospital, located at 467 First Avenue, New York City, with toy guns and steal one of the patients out of the hospital. The Crazies plan to put a strait jacket on one of their own members, sneak him into Bellevue, and then other Crazies with the toy guns plan to enter and steal the patient. B. After they leave Bellevue, The Crazies plan to travel to the Staten Island Ferry and board the boat which travels between lower New York City and Staten Island. They plan to enter the boat peacefully, i.e., paying their way and not jumping over the rail, and when they get on board they plan to threaten the boat's captain by demanding that he take them to Cuba. When the captain obviously refuses to do so, they plan to rush to one side and threaten to 'tip the boat over.' " This is followed by the sobering statement that "Military personnel traveling to New York City often use the Staten Island Ferry."

The Subcommittee on Constitutional Rights found that hundreds of copies of the military's voluminous surveillance files and reports were distributed throughout Government agencies, including NASA. After the Secretary of Defense (then Melvin Laird) ordered, under pressure, the Army to destroy all dossiers on civilians in 1971, the subcommittee unearthed considerable evidence of "deception, cover-up and noncompliance" with the order, indicating that files had sometimes been hidden or disguised. "All of these incidents of deception," the subcommittee concluded in 1973, "indicate that Army intelligence simply cannot be trusted to monitor and police its own system." Nor did the Senators believe that the Department of Defense could be so trusted. Meanwhile, one committee aide points out, "We never did get a chance to look at the files of the other branches of the military. Who knows what's happening there?" Some, such as Representative Moorhead, believe that other Government agencies, such as the Special Analysis Division of the Office of Emergency Preparedness, an agency that until June 17, 1972, employed James W. McCord, Jr., may have "assumed" some of the Army dossiers.

Thomas Powers, commenting on these files in *Atlantic Monthly*, asks, "Are the students who went south on the Freedom Rides, who marched against the war, who protested secret weapons research on

college campuses, who resisted the draft or were beaten by police in Chicago, or who stalked out of commencement speeches by Government officials going to be forced to explain themselves for the rest of their lives? Movements come and go, but the files go on forever."

"The new technology," Senator Sam Ervin stated on the floor of the Senate, "has made it literally impossible for a man to start again in our society. It has removed the quality of mercy from our institutions by making it impossible to forget, to forgive, to understand, to tolerate. . . . The undisputed and unlimited possession of the resources to build and operate data banks on individuals, and to make decisions about people with the aid of computers and electronic data systems, is fast securing to Executive branch officials a political power which the authors of the Constitution never meant any one group of men to have over all others."

[From the New Times Magazine, Oct. 18, 1974]

Reading the Future

John Naisbitt is a pre-computer age George Gallup. His clients, who pay $2,000 a year for the quarterly service he provides, include General Motors, Xerox and the Club of Rome. They pay for his deceptively simple practice of poring over 206 newspapers in 156 cities each day with the aid of 30 staff analysts. Naisbitt is a futurist whose highly respected *Trend Report* both dissects the present and forecasts the future. His prognostications often precede by as much as two years public awareness and media treatment of a social trend.

What follows are just a few of Naisbitt's most recent and most provocative predictions:

—Demonstrations and confrontation politics are coming back and will include job riots in major cities. The seeds, although largely unreported nationally, are in cities where thousands have been turning up for a few advertised jobs, and frustration has turned to ugliness.

—Buildings and cordoned-off neighborhoods will adopt the successful anti-hijacking techniques of the airline industry. In response to increasing crime and violence, entering persons will be X-rayed and frisked despite the offensiveness of the method. Heavy security precautions already being taken by the very rich—bells, guards, fences, electronic barriers and floodlights—are the first rumblings.

—The two party system will soon be dead. Increasing political independence and diversity will spawn not only splinter parties on the left and the right but also special purpose parties comprised of groups such as environmentalists, ethnics and grey panthers.

—Our scale of living will be vastly reduced. Family sizes will shrink, assembly lines will be broken into smaller groups, and the popularity of small towns will return. There will be a more decentralized approach to problem solving and of necessity a recycling ethic will prevail.

—Within a decade the country's largest minority will be Latino (rather than black) and Spanish will be our second language. A number of state governments—including California, Connecticut and Illinois—already issue announcements in both Spanish and English.

[From the Wall Street Journal, Oct. 31, 1974]

Man's Best Friend For Sniffing Bombs May Be a Machine

ELSCINT LTD. SAYS NEW DEVICE DETECTS EXPLOSIVE VAPORS IN 60 SECONDS OR LESS

New York.—Dog lovers may hail it as the savior of animals assigned to seek out dangerously explosive materials, but others are likely to assail it as creating canine unemployment through automation.

That's the "Explosive Detector, G.C.," dubbed by its makers as an automatic "bomb-sniffing" device.

Elscint Ltd., based in Haifa, Israel, demonstrated the 70-pound, suitcase sized device that accurately signaled the presence of a stick of dynamite wrapped in a plastic bag. Besides a "beep-beep" warning and a flashing red light, the machine registered on graph paper the type of explosive it had uncovered.

Amos Linenberg, manager of Elscint's chemistry division and inventor of the device, said it can detect vapors from explosives in the air, in wrapped packages, on the hands of persons who have handled explosives and on vehicles used to transport explosives.

Mr. Linenberg said the machine will signal an amount of vapor "as low as three parts per trillion" in 30 seconds.

The machine, Mr. Linenberg said, can be programmed to detect such explosives as TNT, dynamite and gelignite. In some cases, the device can take "as much as 60 seconds" to record its discovery. So when one is racing against time, it's best to have more than one machine programmed for different types of explosives, he said.

At $12,000 a unit, the inventor said 30 machines have been purchased by various governments, including Eastern European countries. Some are "being used by several U.S. federal governmental agencies," he said.

The level of error of the "Explosive Detector G.C." is "almost zero," according to Mr. Linenberg, who said the vapor traces left by many explosives are long lasting. In certain cases they remain "up to three weeks," despite washing. This may be the weakness of the device, as it will single out as a suspect anyone who may have shaken hands with, say, a "mad bomber."

The machine is useful even after the fact, he said, because it "can determine the specific compound used" by an analysis of debris.

As Mr. Linenberg puts it, the device is "a scientifically accurate replacement for trained dogs."

[From the Los Angeles Times, Oct. 26, 1973]

Scramble the Bugs

(By Art Seidenbaum)

The ad appears in the October issue of the American Bar Assn. Journal. There's a profile of a man with a mouthpiece and the caption reads: "We can't discuss it on the phone. When can I see you?"

The rest of the text begins: "How many times have you put off discussion of sensitive topics, simply because you felt you couldn't trust your telephone?"

Shades of G. Gordon Liddy and other shadowy figures. A Los Angeles County supervisor recently told me he didn't want to offer some information over the phone but he'd be happy to provide it in his office. I know a businessman who likes to leave his plush spaces for a pay telephone to begin certain conversations.

The Ground/Data Corp. of Ft. Lauderdale, Fla., sponsor of the ad, suggests the following solution. ". . . a voice scrambling system that is both highly effective and practical for everyday use. To any intruder who may tap your lines, Ground/Data Voice Sequestors makes both sides of your conversation unintelligible. Yet you and the party you're talking to hear each other loud and clear, whether or not the other person's phone is equipped with a scramble/unscramble device."

It has come to this—electronic debuggery to achieve privacy.

Loyola law school Asst. Prof. Les Rothenberg found the ad a predictable echo of Watergate and figured attorneys are ripe prospects for antitap devices.

And so I called Ft. Lauderdale to find out about any boom in unbugging.

"You'd think Watergate would help the business," admitted Ground/Data Vice President Peter Maitland. "Funnily enough, it works both ways." There are those businessmen or lawyers who feel a new need for privacy, he said. But there are also bosses who now want to know why any of their executives would have to hide any conversations.

Maitland, in a beautifully articulated English accent, said there are about half-a-dozen firms in the scrambling business, Ground/Data being one of the biggest. Their clients include oil companies who live in daily fear of business espionage, especially in matters of resource discovery and leases. They also cater to firms who may be contemplating mergers and who don't want the government to know about the marriages in process.

Government, in the form of the Internal Revenue Service, is feared to be the major American tapping institution.

Maitland would not tell me his firm's revenues for last year but he did say Ground/Data has been in the scrambling business for three years and the market for unintelligibility is growing.

I asked him whether our conversation was being scrambled for any possible intruders at that time. No, he said. What would it sound like if it were, I wondered. Noise, he said. Their high-security system carries no intelligence at all.

Ground/Data and its legitimate competitors have their own security problems, in terms of keeping such sophisticated systems out of the mouths of the Mafia. Maitland said they must be extremely careful in screening clients and also in assuring respectable clients that Ground/Data will never operate as a double agent—scrambling for one customer and unscrambling the same messages for another rival customer.

So humankind has tap devices and antitap devices and anti-antitap devices. Our ingenuity being infinite, keeping complete security is possible only by keeping no secrets.

[From the Washington Post, Nov. 24, 1974]

Thirty Lessons for an Easier Watergate: Do It Yourself

Anyone who wants to pull his own Watergate can learn how for less than $10.

An organization calling itself the Police Electronics Institute sells a simple, do-it-yourself wiretapping and electronic eavesdropping manual that promises to teach "how experts earn $40,000 to $100,000 per year."

The manual cautions that the wiretapper's trade is illegal but offers this observation: "The illegal tapper, like the speeding motorist, takes his chances, but the tapper's gamble is generally more lucrative."

While government officials say it is legal to distribute eavesdropping and wiretapping information, it is illegal for private individuals to possess or use bugging or wiretap equipment. And the head of a government investigation of wiretapping expressed concern that easy access to such information will encourage private citizens to break the law.

The Police Electronics Institute has a Chicago address that appears to be only a mailing point for persons ordering the 30-lesson manual, costing $9.95.

The institute is not listed in the Chicago telephone directory, and police there said they have never heard of the organization. They describe the mailing address as "a two-family flat on Chicago's North Side."

Called the "Electronic Investigation and Secure Communications Course," the manual states in the beginning that "regardless of restrictions against bugging and wiretapping, there will always be those to whom obtaining information is more important than the risk involved."

In response to its own question in the first lesson, "How Do You Become a Wiretapper?" the manual states: "Paradoxically, one can start in this highly paid profession with no training whatsoever. No electronic experience is required to start."

What follows are some 90 pages of definitions, descriptions, diagrams and uses for various wiretap and bugging devices, as well as detailed instructions on how to install them in telephones, rooms and automobiles.

For the inexperienced tapper, the manual offers this warning: the bugged martini olive, a tiny transmitter designed to look like an olive, will "not work while immersed in a martini."

The manual claims that would-be tappers are not the only ones who would benefit from buying the book and suggests that anti-tap security experts also would gain.

"To do the anti-tap work, you must have the knowledge of the tapper and be able to think like a tapper," the manual says.

For this reason, "The point of view of the manual often approaches the subject from the point of view of the tapper," the manual says.

The manual claims the course is "offered to individuals involved with or about to enter law enforcement, security work or allied fields." Yet, when a private citizen wrote for a manual, no check was made to see why he wanted it or how he would use the information.

A government official says he is concerned about this easy access.

"The problem is there is apparently no control on whom the book is sent to," said Michael Hershman, chief investigator for the National Wiretap Commission, a government agency created to study wiretaps. "What they're doing is planting information in the hands of individuals who very well might use it to break the law."

Hershman, a former Senate Watergate Committee investigator, is now in charge of evaluating the government's electronic laws. "The book makes it easy to build and utilize electronic devices," he said. "And we have no idea how many people have access to this information."

[From the Wall Street Journal]

"Debugging" Experts, Aided by Watergate, Detect Rise in Sales

Customers fear eavesdropping by competitors or spouses; the fluorescent secretary

(By M. Howard Gelfand)

Chicago.—The businessman is nervous, and he isn't taking any chances. He pushes a button under his desk, and the mahogany office doors slide closed. Then he turns to face Ed Bray: "I checked you out with some friends, and they say you're okay, but in this business you've got to know who you're dealing with. Let me see your wallet."

After a brief inspection of Mr. Bray's identification cards, the man nods his satisfaction.

"What's your price?"

"One thousand dollars," Mr. Bray answers. "And we deal in cash up front."

The businessman nods again. Hard-talking Eddie Bray, a former Chicago policeman who now heads American Security Agents Inc., a private detective agency, has made another sale.

What Mr. Bray sells is "debugging"—the detection of devices used to eavesdrop on conversations. Business is good. Thanks in large part to the Watergate scandal, public awareness of bugging and the demand for debugging service are growing, those in the field say.

Just how many people are the target of electronic surveillance isn't known. The American Civil Liberties Union estimates that since 1968 the federal government alone has bugged 150,000 to 250,000 persons suspected of various offenses. Many more have had their phones or offices wired by business competitors, estranged spouses and the like.

The gray box

All that activity has brought a technology boom to both the science of bugging and the science of debugging. Microphones that pick up conversations have been miniaturized to the extent that they'll fit into light fixtures, electrical outlets and scores of other out-of-the-way places.

Debugging experts say their best weapon is a meticulous search of the premises. Such big security firms as Pinkerton's Inc., Wacken-

hut Corp. and Burns International Security Services Inc. might spend an entire day searching a business office, looking behind ceiling boards, tiles, carpeting and flooring and removing and examining light fixtures and other ornaments. Some even use an X-ray machine to make sure a bug hasn't been planted behind a wall.

But all that is time-consuming and expensive, especially considering the fact that a bug is only rarely discovered. "It's the seat-belt syndrome," says Allan D. Bell Jr., president of Dektor Counterintelligence & Security Inc., a Virginia concern specializing in security technology. "The guy who wears a seat belt is the same sort who usually calls us in. He is so cautious that he probably isn't in any danger. It's the other kind of guy who gets in trouble."

Thus, investigators such as tough, rough Eddie Bray increasingly are using detection devices that do the job quicker and cheaper, although admittedly not as thoroughly. Mr. Bray uses a 3½-pound gray box equipped with a red light that glows when a radio signal is received. It takes him about 15 minutes to rotate a small black dial that scans every part of the low and high radio frequencies. The device is equipped to receive any signal sent from a bug. He charges $100 per room and $100 per telephone line for the procedure.

"THE FEDS GOT YOU WIRED"

On the rare occasions when Mr. Bray detects a listening device, there often isn't much he can do about it. In the case of the nervous businessman, Mr. Bray's receiver picks up a transmission from a bug, but he concludes it is in the phone lines in the alley behind the man's office.

"The Feds got you wired," Mr. Bray triumphantly announces to his client, who is under investigation in a criminal matter.

"I thought so." is the reply. "The phone company had its trucks out in the alley all day yesterday."

"I'll tell you what you do," Mr. Bray says. "Wait a day or two. Then call a friend who's absolutely clean. Tell him, 'Joe, I just found out the G-men have my phone wired.' After they know you know you're bugged, they'll probably remove it." Sure enough, when Mr. Bray returned two weeks later, the bug apparently had been removed.

More commonly, his clients fear industrial, not government, spying. Mr. Bray recently spent 15 minutes in the office of a corporation president who was guarding the secret of a copying machine he had invented. Although Mr. Bray didn't find a bug, the case reminded him of a similar job on which he "hit the jackpot"—he found a bug under the desk of a contractor who was consistently being slightly underbid by a competitor. Mr. Bray suspected the man's secretary had planted the device and was changing its batteries, so he rubbed some invisible fluorescent powder on the bug.

Then he waited until the secretary had been alone in the office. When she emerged, he ushered her into a room in which he had installed a black light. When she stepped under the light, the powder glowed, and the case was solved.

Lately, however, many of Mr. Bray's clients have been politicians. When the U.S. Attorney here announced he was investigating 10 unnamed aldermen in an influence-peddling scheme, "the phones were

ringing off the hook all day," says Joseph Paolella, Mr. Bray's partner and an ex-FBI agent. Asked if 10 of the city's 50 alderman called Mr. Paolella laughed: "Ten? I think they *all* called."

Mr. Bray, who earned $40,000 last year, must endure certain occupational hazards. While he insists that he wants nothing to do with gangsters, it's nevertheless a fact that some of his clients are the sort of people who have their mother-in-law start their car for them in the morning.

"A man is innocent until proven guilty," Mr. Bray solemnly intones. His translation: "If he's under indictment, we'll take him."

Another burden debuggers must bear is their image problem. Anyone with a private investigator's license can hang out a debugger shingle. As a result, some inexperienced and incompetent private eyes are said to be exploiting the paranoia stemming from the Watergate scandal. "People are willing to buy a pig in a poke," says Mr. Bell of Dektor, "and there are a lot of people who sell pigs in pokes."

Samuel W. Daskam, an electrical engineer and general manager of F. G. Mason Engineering, a Connecticut firm that sells and operates debugging equipment, tells of watching one imposter at work. "He had a little black box with a red and a green light attached to it. The inscription above the lights was, 'If it's green you're clean, if it's red you're dead.' He plugged it into the guy's phone and the red light went on. Then he said that by throwing a switch he'd 'burn out' the bug. He threw the switch, and the green light went on. I wish," he says, "it were that easy."

Then there's the fact that anyone who can detect a bug can plant one. In many places, debuggers aren't even allowed to advertise in the Yellow Pages. As the Missouri Public Service Commission put it recently: "Advertising the ability to detect and remove electrical devices was, in fact, also advertising the ability to plant those same devices."

This is an assertion that especially saddens Mr. Bray. "Don't even talk to me about planting a bug," he protests. "Life is too short. I'm doing too well. I don't need that."

He checks his own office telephones several times a week, although he found a bug only once. "Joe and I had a pretty good idea who was doing it," says Mr. Bray. He won't say what he did about it, but he grins with obvious delight when he says, "We made sure it wouldn't happen again."

[From the Washington Star, March 26, 1975]

D.C. Police Plan for Drinking Drivers: A Very Candid Camera

(By Toni House)

If you're one of those persons who's inclined to combine drinking and driving in the District, you'd better start brushing up on your alphabet.

Starting in mid-April, reciting the alphabet is just one of the little exercises persons suspected of drunk driving will be asked by police to perform—for a video camera.

Time was when walking the straight line painted in front of the sergeant's desk at the stationhouse was the accepted test of a driver's sorbriety.

While primitive, the old straight-line test is in the family of so-called "cycle-motor" tests—including reciting the alphabet—Washington police will be using and recording on video tape in its soon-to-be-launched war against drunken drivers.

And a warning to the two-fisted drinker who thinks his power of concentration can overcome the police department tests. An assistant corporation counsel with a similar attitude recently consumed several drinks under the eye of the police and when he was statistically drunk tried to outsmart the cycle-motor tests. In four tries he never got past the letter "g."

In a pilot program to begin April 18, a special team of Traffic Division officers will go on the prowl in target areas, armed with the latest in portable videotape equipment and, in another first for the city, a Breatholizer to test on the spot the alcohol content in a driver's blood.

If the program proves successful, the department hopes to equip eight cruisers with the mini-television cameras and microphones and provide Breatholizers for each stationhouse.

When the teams get rolling Washington will be the third jurisdiction in the United States to use videotape on the street. While 19 other police agencies use videotape, most keep it in a central location and take the suspect to it. With an on-the-street program, Los Angeles County has a 98 percent conviction rate in drunk driving cases, police said.

Police already have applied for a grant from the U.S. Department of Transportation to finance a citywide project for three years.

Until now, District police, who have had what they consider an unacceptably low conviction rate in drunk driving cases, have utilized "crimper" tubes to test a driver's breath. But after a breath sample is taken in a tube, it has to be shipped to a laboratory for analysis, a slow and chancy project, police said.

The Breatholizer, already in extensive use elsewhere, tests a driver's alcohol blood level immediately. As a driver breathes into the machine, it instantly analyzes it and prints out a card used as evidence in court. If the driver "blows" at .1 percent or higher, he is considered legally drunk.

The video tape, police said, is to add weight to the breath test, to fend off pleas that the defendant was not "really drunk."

Police said such a simple rote exercise as reciting the alphabet becomes difficult for someone who has drunk too much. Most cannot get beyond the letter "g" without some problem. The letter "q" seems to be a real stumbling block for the drink-thickened tongue, according to police.

Suspects also will be asked to count to five and to walk a straight line and talk at the same time. Neither is easy, police said, if you're under the influence.

The District's program differs from the highly publicized, federally funded ASAP program in neighboring Fairfax County.

The Fairfax program, which has nabbed nearly 11,000 suspects since it began over two years ago, is a joint rehabilitative effort among police, probation officers and the courts.

At present, there are no similar programs in the Maryland suburbs, although police do have personnel trained and available to use the Breatholizer machine. In Montgomery County, for instance, there are trained operators assigned to each police station. Until Jan. 1, Maryland state police had a special enforcement unit to detect and arrest intoxicated drivers, financed by a federal grant, but it was discontinued for lack of further funds.

The thrust of the new D.C. program is enforcement and prevention rather than rehabilitation, Traffic Division Deputy Chief Ernest J. Prete said. He said police here plan to make it so hot for potential offenders that they'll have to choose between driving and drinking. The little town of Covina, Calif. (population 32,400), which also uses on-the-street videotape, has lost only one case out of 1,200 in court. In self-defense, the bar owners have bought a bus to transport inebriated customers, police said.

[From Parade Magazine, Mar. 30, 1975]

FBI's Air Force

The Federal Bureau of Investigation has started building its own air force, purchasing two specially designed aircraft originally built for clandestine nighttime surveillance during the Vietnam war.

Television viewers who followed the FBI's exploits through a semi-fictionalized Sunday night series popular for many years probably thought the bureau had an air armada because the agents portrayed in that program regularly used helicopters and light planes for aerial chases, surveillance and various other purposes.

In fact, the FBI had never owned any aircraft. On occasions when planes or helicopters were needed for special assignments, they were leased from other government agencies or commercial chartering companies.

Several months ago, however, the FBI bought two surplus reconnaissance planes initially constructed for the Army by the Lockheed Aircraft Corp.

The new FBI planes, officially designated the YO–3A, look very much out of place in the era of supersonic jet aircraft.

In Vietnam, the Army wanted a plane so quiet that it could not be detected by Vietcong troops on the ground even when it flew at an altitude as low as 100 feet.

Given that order, Lockheed began with a glider frame whose huge wings would allow it to soar for long periods without requiring much power. For a propulsion system, the company initially installed a 100-horsepower engine. In later models, the size was increased to 200 horsepower, but even that is astoundingly small when compared with the 300- and 400-horsepower engines in many passenger cars.

A thick layer of insulation was wrapped around the engine to muffle the noise. Then Lockheed went back to the earliest days of aviation for a six-bladed propeller made of wood, which makes far less noise than metal when it bites into the air.

Finally, the plane was outfitted with highly sophisticated nighttime sensing devices which could track troop movements in the jungle. Development of the special plane cost the Army an estimated $10 million.

Rep. Les Aspin (D., Wis.), who discovered the sale of the surplus military aircraft to the FBI, has criticized the purchase on the grounds that "the FBI has provided absolutely no justification for establishing its own air force." The Congressman has protested the sale to FBI Director Clarence M. Kelley, alleging that "the bureau ought to get out of the air power business as soon as possible."

But the arrangement has been defended by William Sullivan, special agent in charge of the FBI's Los Angeles field office, where the two planes will be based and used for aerial reconnaissance in a seven-county area of Southern California.

"It's strictly an experimental thing," said Sullivan. "But we think the plane could be very effective in trailing cars involved in extortion or kidnapping plots, for example, or in rescuing kidnapping victims."

Sullivan said he'd like to experiment with nighttime surveillance, using the sensors developed by the Army. He emphasized that the plane will be used for "investigative purposes only," not for transporting government employees.

[From the New York Times, Jan. 22, 1974]

Police Zoom In on Pushers With New Camera Tricks

(By Edith Evans Asbury)

In an attempt to build more effective cases against dealers in illegal drugs, the Police Department is training narcotics detectives to use sophisticated cameras and electronic devices.

One class has already been graduated and another will begin next month to learn how to use the one and one-half million dollars worth of cameras—still, motion picture and television—and lenses—near and far, day and night—bought for their use.

Dramatic results have already been produced by detectives using the photographic and electronic equipment, according to Assistant District Attorney Frank Rogers, the city's special narcotics prosecutor.

"When you show a defendant a photograph of himself making the sale he is accused of, he is devastated," Mr. Rogers said. "We are getting a lot of guilty pleas."

Special measures to insure solid cases against narcotics operators became necessary after the disclosure of police corruption at Knapp Commission hearings, and the disappearance from the Police Department Property Office of $73-million worth of heroin and cocaine that had been seized in the "French Connection" case.

Credibility of narcotics officers was severely damaged by the revelations. Skeptical juries often refused to convict when the principal evidence was testimony by a police officer. This reluctance by juries was intensified by legislation which went into effect last August mandating harsher penalties for those they found guilty. At the same time, the harsher penalties meant that more defendants would demand jury trials.

Sgt. James Sottile, himself a former narcotics detective and a amateur photographer, organized the new training program and supervises it.

Members of the classes were selected from narcotics divisions throughout the city, with preference given to those who had already demonstrated interest and proficiency in photography.

To obtain materials for classroom use, Sergeant Sottile sent members of the first class out to photograph, from a variety of locations, typical sites of drug operations—streets, parking lots, doorways, rooftops.

At the same time, the detectives also learned about expanded surveillance possibilities possible with the camera. They took long-range photographs from helicopters and high buildings, then zoomed in with lenses that produced details such as identifiable faces and automobile license numbers.

The detectives also learned to take surreptitious pictures with wide-angle lenses that could photograph a whole room from close quarters.

From concealed stationary positions, such as a church steeple, an apartment window, a parked van, the detectives recorded street scenes with motion picture and still cameras.

Polaroid cameras were used to photograph fingerprints, marked currency, such as would be used for undercover drug purchases, pictures of suspects and other documents.

Assistant District Attorney Rogers, who asked for the special equipment and training when he took over prosecution of narcotics cases for the city, said last week that photographic evidence, as well as evidence taped by videotape, body recorders and other electronic devices, has helped raise his office's conviction rate from 50 per cent to 80 per cent.

One defendant, after being shown a television recording of herself going into a bar to make a drug purchase and coming out with it, agreed to provide information about her source of supply that has resulted in the conviction of many other persons, Mr. Rogers said, with still more to come.

[From the Los Angeles Times, Apr. 10, 1975]

Twenty-three U.S. Agencies, From Mapping Unit to IRS, Spy on Citizens, ACLU Alleges

(By Linda Mathews)

Washington.—The American Civil Liberties Union said Wednesday that at least 23 separate agencies, ranging from the FBI to the Defense Mapping Agency, were conducting electronic surveillance of American citizens.

The ACLU based its conclusion on government affidavits produced last month in the West German court-martial of a young Army lieutenant charged with letting his hair grow too long. But the ACLU, which had defended the lieutenant, waited until Wednesday to release the list.

Besides the FBI, the list identified the Central Intelligence Agency, the Internal Revenue Service, the U.S. Postal Service and the Secret Service as among the agencies which engaged in wiretapping and bugging.

Also included were more obscure arms of the federal government with less obvious investigative functions, such as the Defense Mapping

Agency, the Defense Contracting Audit Agency, the Army Criminal Investigation Command and the administrative services section of the Joint Chiefs of Staff.

The government affidavits on which the ACLU list was based did not explicitly admit that each agency had eavesdropped. But in each case, the agency had said that records of electronic surveillance had been examined in drawing up the affidavits.

The government's disclosures led Charles Morgan Jr., director of the ACLU's Washington office, to charge that then-Atty. Gen. William B. Saxbe lied under oath last year about the scope of government eavesdropping.

Morgan referred to Saxbe's testimony at joint hearings of three Senate subcommittees last May 23, where he indicated that the FBI was the only government agency engaged in electronic surveillance.

In one exchange during those hearings, Sen. Edward M. Kennedy (D-Mass.) told Saxbe: "What we are trying to find out is whether there are any governmental agencies which are involved in any wiretapping whatsoever."

"The answer, to the best of our knowledge, and we have made diligent search, is no," Saxbe replied.

"For all agencies of government?" Kennedy asked.

"Yes, sir," Saxbe said.

Kennedy pressed further, saying, "You can give that authoritative statement that there is no agency of government in the United States which is involved in electronic surveillance today?"

Again, Saxbe's response was, "We have made diligent search."

"Other than the FBI, is that correct?" Kennedy said.

"That is correct," Saxbe said.

Earlier in the same hearings, Kennedy referred to former President Richard M. Nixon's then-recent disclosure that the Secret Service wiretapped his brother, F. Donald Nixon, and quizzed Saxbe about whether the Secret Service had done further wiretaps.

"No," Saxbe said.

"And the CIA?" Kennedy asked.

"No, sir," Saxbe said.

"How about Army intelligence?" Kennedy said.

"No," the attorney general answered.

Although the senator clearly asked about all the wiretapping activity of government agencies, there were indications in the transcripts of the hearings that Saxbe and FBI Director Clarence M. Kelley may have thought that the inquiries concerned only surveillance carried on without a judicial warrant.

The Justice Department long has maintained that the attorney general, acting under the President's inherent authority to protect national security, is empowered to authorize some wiretaps without first obtaining the approval of a federal judge.

This contention met partial defeat three years ago in the Supreme Court, which ruled that national security cannot be invoked as an excuse to bypass normal warrant procedures where antiwar activists and other so-called "domestic subversives" are concerned. But the justices explicitly reserved for future resolution the question of whether warrants could be dispensed with when the government suspects foreign espionage.

The high court's action means that some warrantless wiretapping remains at least arguable constitutional, until the justices rule definitively on the question.

During the Senate hearings, both Saxbe and Kelley occasionally focused on wiretapping conducted without a warrant. Their remarks could be taken to mean that it was only this kind of surveillance that was confined to the FBI.

Saxbe, for example, testified that he had "put out a questionnaire" to various agencies to find out the extent of their eavesdropping.

"Where we were concerned was on the national security level," Saxbe explained. "We were concerned that . . . perhaps the Secret Service, perhaps CIA, perhaps the Department of Defense, were running national security surveillance. The answer is, no."

Earlier, Kelley had pointed out that the 1968 Omnibus Crime Control and Safe Streets Act permitted other federal agencies besides the FBI to seek judicial warrants to wiretap in connection with investigations of a long list of specified crimes. "Under (this act), there are some other agencies which seek and secure that right," Kelley testified.

Among the crimes for which wiretap authorization can be obtained, under the 1968 law, are presidential assassinations and assaults, various drug offenses, murder, kidnaping, robbery, bribery of public officials, theft and racketeering.

Most of these fall clearly within the jurisdiction of the FBI, which would mean that it should be the only agency conducting surveillance of those crimes, with or without warrants.

But, for several crimes listed in the act, the FBI shares responsibility with other federal agencies identified by the ACLU as active in eavesdropping. The Secret Service, for example, is charged with protecting the President and could be said to have acted properly if it obtained warrants to eavesdrop on would-be assassins. Similarly, the Drug Enforcement Administration could properly keep suspected drug offenders under surveillance.

It was impossible to tell late Wednesday whether, in fact, the eavesdropping activities of each agency had been tailored to its special interests. The ACLU list merely identified the bodies that engaged in snooping and did not disclose the extent or nature of those activities.

The ACLU compiled the list from affidavits made available to an affiliated attorney in Heidelberg, Germany, H. Christopher Coates, who had been representing Army 1st Lt. Matthew R. Carroll at a general court-martial.

Before charges against Carroll were dismissed because of an unrelated technicality, the Army had been ordered to disclose whether any of its agencies had eavesdropped on Carroll or two stateside ACLU attorneys, John H. F. Shattuck and David F. Addlestone, who had been helping with his defense.

What the government produced was a heavy sheaf of affidavits from officials in 23 different agencies, saying that they had searched their electronic surveillance records and could find no evidence that the three men had ever been wiretapped or bugged.

The ACLU took that to mean that all 23 had at some time engaged in electronic surveillance and distributed to reporters the list it had drawn up, accompanied by copies of the affidavits which ran 28 pages long.

Beside the agencies already named, the following were listed as participating in some eavesdropping activities.

The National Security Agency; the Treasury Department's Bureau of Alcohol, Tobacco and Firearms; the Naval Investigative Service; the Defense Intelligence Agency; the Defense Nuclear Agency.

Also, the Defense Security Assistance Agency; the Defense Supply Agency, the Defense Civil Preparedness Agency; the Defense Advance Research Projects Agency; the Defense Communications Agency; the Defense Investigative Service; and the Department of the Air Force.

Under the Department of the Army, three small units were named: the 502d Army Security Agency Group; the Office of Deputy Chief of Staff for Intelligence, U.S. Army, Europe; and the Investigation and Police Information Division, U.S. Army, Europe.

The State Department's Office of Security was listed as receiving surveillance information from other agencies but not conducting its own.

[From Newsweek Magazine, Apr. 14, 1975]

Electronic Fire Spotter

For hours, dense clouds of potentially lethal hydrochloric acid gas had spewed from a leak in a million-gallon industrial chemical tank on the Chicago docks. Scores of firemen in gas masks and protective clothing fought the gas as best they could by neutralizing the spilled acid with slaked lime, but as the cloud increased in size and opacity (at one point it covered an area of 10 square miles), it became impossible for the firemen to determine how much acid had been spilled—and how much lime they would need to complete their task.

Finally, fire-department officials put in an emergency call to the Hughes Aircraft Co. in California. Several hours later a Hughes technician arrived by plane with what at the time was a largely experimental device called a Probeye. The Probeye detects objects by sensing the infra-red rays they emit. Using the Probeye, firemen quickly determined the level of chemical in the leaking tank (the chemical was known to emit a higher intensity of infra-red rays than either the tank or the atmosphere surrounding it) and dumped the required amount of lime on the spill. Afterward, they used the Probeye to scan the ground in the leak area for remaining traces of the acid.

Infra-Red: What the 7¼-pound Probeye does is convert infra-red radiation from objects in front of it into relatively sharp images on a tiny television screen. It was first developed three years ago for use in Vietnam to locate enemy troops at night by picking up the infra-red rays emitted by the human body. Not long thereafter, Hughes technicians began adapting it for use by fire fighters, who now consider it as an invaluable piece of equipment.

In a smoke-filled room, for instance, a human body is seen in striking contrast to its surroundings. Trained experts can use the device to distinguish hair, clothing and in some cases even the air exhaled by trapped victims. If a room is aflame, technicians can detect a body by scanning the area from different angles until they get a view of the body in front of the flames; in cases like this, the body appears as a

79-064 O - 76 - 63

dimmer outline against the greater intensity of the infra-red rays emitted by the flames. The Probeye is also used to detect short circuits and other likely sources of fire that may be concealed behind the walls or above ceilings. So far, Probeyes are in use by twenty fire departments across the nation, and the firemen report only one real problem—local police departments are constantly borrowing them to detect nighttime prowlers.

[From the Washington Post, Apr. 24, 1975]

U.S. Probes Agents' Role In Wiretaps

(By Ronald Kessler)

Houston.—U.S. prosecutors are investigating charges that federal agents participated with Houston police in illegal wiretapping.

Houston Police Chief Carroll M. Lynn and former U.S. Attorney Anthony J. P. Farris said in separate interviews that the charges have been made by present and former Houston police officers, some of whom admitted they had personally conducted the illegal activities with the assistance of the telephone company.

The allegations of federal participation, made in investigations conducted by Lynn and Farris, involve the Drug Enforcement Administration, both men said.

To a lesser extent, Farris said, the FBI is alleged to have conducted its own illegal wiretaps.

The facts concerning this charge are hazy, Farris said. Other sources said the FBI is also alleged on at least one occasion to have participated with police in illegal wiretapping and to have been aware of the illegal practices by police without taking any action to stop them.

The allegations are being investigated by the U.S. attorney's office here. Farris, who left that office last December to enter private practice, said the probe has depended on the FBI to investigate fellow law enforcement agencies—including itself—the bureau has reacted with a "lack of enthusiasm."

Farris, who was U.S. attorney for six years, said the FBI said it lacked manpower, and assigned two agents to work on the case part-time, although as many as 50 Houston police officers allegedly were involved.

The agents' reports were "ridiculous," Farris said. "Some covered one page—others covered 10. They were repetitious, skeletal, and included Xerox copies of newspaper articles. Well, hell, I had read all those."

Farris said he complained last November to then Attorney General William B. Saxbe about what he termed the Justice Department's lack of concern about the case.

The complaint, a six-page letter with exhibits, pointed out that some of the allegations being investigated involved the FBI and said the FBI effort in the case was "not there," Farris said.

Farris said he received no reply.

Spokesmen for the Justice Department and FBI declined to comment because the matter is being investigated by a grand jury. A DEA official said the charges involving the drug agency are "not true."

The federal investigation in Houston began after the Internal Revenue Service obtained indications that Houston narcotics officers who were selling heroin seized during police investigations were also using illegal wiretaps to obtain arrests.

Nine present or former officers were indicted last year for tax evasion or wiretapping as a result of the investigation.

The Houston investigation began receiving national attention late last year after the telephone company executive in charge of Texas operations charged in a suicide note that the company was conducting illegal wiretapping.

In recent interviews, Farris and Lynn said officers who have admitted to wiretapping have alleged they were given information necessary to install each wiretap from the security office of the local American Telephone & Telegraph Co. subsidiary, Southwestern Bell Telephone Co.

In some instances, Lynn said, the security office allegedly returned illegal wiretap devices found on telephone lines to the police department.

One of the nine indicted police officers said in an interview that he personally obtained wiretap information from the telephone company security office about a half dozen times. He said the security office also provided him with records of long-distance toll calls.

Jerry L. Slaughter, a former FBI agent who heads the security office, did not return telephone calls. However, a company spokesman said he has previously denied the charges.

The spokesman said the company cannot deny that someone in the company might have helped police wiretapping, because the company cannot speak for each of its 14,000 employees. But he said such actions are against company policy, and would result in dismissal if substantiated.

The Southwestern Bell allegations have been under investigation by a number of federal authorities, including the National Wiretap Commission and the House Judiciary Subcommittee on Administration of Justice, headed by Rep. Robert W. Kastenmeier (D-Wis.).

Kastenmeier's subcommittee last week obtained some of the evidence being used in the federal investigation in Houston. The evidence consists of transcripts and tape recordings of informal conversations between Lynn and some of his aides and officers shortly after he took over as police chief early last year.

According to a source who has read the transcripts, the officers freely discussed the illegal practices, unaware that Lynn was secretly tape-recording them.

Although federal law permits police officers in most states to wiretap if they can prove to a judge that they have probable cause to believe a crime is being committed, Texas has no state law that would permit such wiretapping. Under the federal law, a state must enact such legislation before police can wiretap legally, according to Michael J. Hershman, chief investigator of the National Wiretap Commission.

In the transcripts, the officers suggested that Lynn should not worry about the federal investigation of the police department because federal agents had participated in the practices or were at least aware of them, the source said.

"The flavor was we had this bunch of boys who did anything they wanted to," the source said.

In court hearings that have not been reported by the press, lawyers representing accused wiretappers have charged that the alleged federal involvement in the wiretapping has impeded the investigation.

One of the lawyers, Dick DeGuerin, a partner with well known criminal lawyer Percy Foreman, said recently that two Houston policemen who were willing to implicate federal agents were indicted by the federal prosecutors after they admitted wiretapping in exchange for immunity on the local level.

DeGuerin said the federal prosecutors said they had valid, legal reasons for not granting the officers immunity in exchange for their testimony.

"My opinion is that they are covering up and don't want to know what went on," he said.

Former U.S. Attorney Farris defended the decision not to grant immunity to the two officers as proper.

However, Farris acknowledged that concern has been expressed in local law enforcement circles that if the full story came out, lawyers could allege in hundreds of cases that their clients were sent to jail on the basis of evidence obtained illegally.

[From the New York Times, June 24, 1975]

Police Said To Own Devices Illegally

Washington, June 23 (AP).—Several manufacturers sell wiretapping and bugging devices to police departments in states where possession of such devices is illegal, even for the police, according to data acquired by the National Wiretap Commission.

Commission investigators have obtained sales records that show that at least three of the largest makers of electronic surveillance gear restrict their sales to Government agencies or state and local law enforcement officers.

Federal law permits the police to own the equipment if they are permitted to use it by state law. However, at least 19 states do not have such authorizing laws.

Among the records examined by the commission were those of the Bell and Howell Communications Company, Audio Intelligence Devices and B. R. Fox Company, Inc. An analysis of the records shows that nearly half of all the devices sold for use in wiretapping phones or bugging rooms go to police in states where possession of such devices is illegal.

The states are Alabama, California, Idaho, Illinois, Indiana, Kentucky, Louisiana, Michigan, Mississippi, Missouri, Montana, North Carolina, Ohio, Pennsylvania, Tennessee, Texas, Utah, West Virginia and Wyoming.

[From the New York Times, June 26, 1975]

Private Detectives Are Found To Offer Illegal Wiretap Advice

Washington, June 25 (UPI).—A random check of 115 private detective agencies in seven cities turned up 42 that either had offered illegal wiretap service or had advised how it could be obtained, the National Wiretap Commission reported today. Congress established the commission to advise it on any needed legislation on electronic surveillance.

In investigating the agencies a commission staff member would telephone those listed in the telephone book's yellow pages tell the investigator that the caller was a local businessman who suspected he was being bugged by a competitor.

The report said that 71 of the 115 firms had offered to debug the offices—clear them of any hidden microphones or other electronic surveillance devices. Many of the firms that refused to install wiretap devices were willing to explain how it could be done by the caller, the report said. The commission released the report amid a series of hearings it was conducting on the extent of illegal wiretapping and bugging in the country. The survey was conducted last April.

Earlier, manufacturers of wiretap and bugging equipment called for stronger laws to keep their sophisticated devices out of the hands of private detectives, husbands spying on wives, company espionage agents and the police who use them illegally.

The 1968 Omnibus Crime Control Act limits the sale of devices for eavesdropping that only the police can conduct lawfully, usually with a court warrant required. But industry spokesmen said that loopholes in the law were so wide that private citizens, company agents and the police bent on illegal investigations could buy them.

In testimony during the wiretap commission hearings, manufacturers' spokesmen called for licensing both makers and users of the equipment. Without this regulation, they said, the present ambiguities in the regulations will continue to make it hard for them to keep the devices from persons ineligible to have them.

The commission report on cities indicated that 18 of 28 agencies in Atlanta had offered debugging services and 14 had offered illegal bugging services. In Baton Rouge, La., five of nine offered debugging and four offered bugging services. In Philadelphia, 20 of 27 agencies offered debugging, 11 offered wiretapping and bugging and three who would not wiretap or bug referred the caller to agencies that would.

In Washington two of nine agencies were willing to wiretap and bug. In Miami four of seven agencies would debug and two indicated that they would wiretap and bug.

In New York six of eight agencies would debug and three offered to assist in wiretapping and bugging. In Los Angeles 16 of 19 would debug but none would provide electronic surveillance.

Some of the agencies contacted offered specialized services and did not deal with wiretaps at all. And some of the agencies would not perform bugging services themselves, but said that they would be willing to offer advice on how it could be done.

[From the Washington Star, Aug. 12, 1975]

Wiretap Seminar for Police

Houston.—The Houston Post said in its editions today that Texas police officers apparently have been taught how to wiretap at out-of-state schools with federal funding.

The Post said records of the criminal justice division of the governor's office indicate this.

The story said records show the Texas department of public safety organized crime intelligence unit was authorized to spend federal funds to send eight agents to an "intelligence officers training seminar" conducted by Bell and Howell Communications Co., a major manufacturer of electronic surveillance equipment, at Miami Beach, Fla., in November 1971. The Post quoted a department spokesman as saying the agents did attend.

[From the Washington Star, Nov. 24, 1975]

Wiretap School Bared by Paper

Chicago (UPI).—A school operated by a subsidiary of the Chicago-based Bell & Howell Co. taught law enforcement officers—some of them from states where wiretapping is illegal—how to use wiretapping equipment, the Chicago Sun-Times reported yesterday.

The newspaper said a federal wiretap commission discovered the Bell & Howell Communications Co., Waltham, Mass., also sold sophisticated eavesdropping equipment to police agencies that cannot legally use the equipment.

The wiretap commission, which conducted hearings in Washington last summer, turned over to the Justice Department several Bell & Howell sales vouchers that reflected the purchases by police and other governmental agencies, the newspaper said.

[From Newsweek Magazine]

New Tools for Cops

Few branches of criminology are more fascinating to police and laymen alike than the research and development of ever more sophisticated hardware designed to make law enforcement quicker, easier and less dangerous. At the annual conference of the International Association of Chiefs of Police in Washington, D.C., last week, the most popular attraction was a $3 million display of the latest in police tools. They ranged from a hand-held radar pistol that tells police if a car is speeding, to a voice-scrambling system that makes interception of spoken messages virtually impossible.

Some of the fashionable new equipment is a direct spin-off from field equipment developed during the Vietnam war. Night patrols in the dark jungle led to the Star-Tron, a kind of telescope that emits no light but is equipped with an interior light-intensifier tube. A policeman carrying a Star-Tron (which costs from $3,000 to $5,000

depending on size) can peer into dark alleys and windows without being seen. Another military-type device is a 148-foot-long bomb-defusing multi-wheeled cart. With a Rube Goldberg array of cables and pulleys, suspect bombs are placed in a fiberglass basket that looks like a giant trash can; when the bomb is detonated, the basket acts as a chimney to drive the force to the blast upward, thus nullifying the effects of both concussion and fragmentation.

Perhaps the most awesome weapon in the police arsenal is the V–150 Emergency Vehicle, an $80,000 tank that was shown by the Louisiana State Police, the first department to own one. It is plated with quarter-inch steel and uses a Chrysler 361 V–8 engine to travel 50 mph on land and 3 mph through water. The V–150 is equipped with first-aid supplies and can rescue people from floods; its crew carries M–16 rifles.

PUNCH

Police technologists have also made broad use of computers. With a unit called Modat mounted in a squad car, a patrolman can punch in the license tag of a car or the name of a suspect—and within seconds receive information from a state data bank or the National Crime Information Center in Washington telling him if the car is hot or the individual wanted for a crime. Some manufacturers have even tried to update such prosaic items as pistol targets. A number of them resemble pop-art cartoons, and depict ordinary people as well as dangerous criminals—hopefully to teach the cops caution.

[From New Scientist, June 12, 1975]

TV Camera for Iran Sees 11 Km at Night

Low light level TV cameras that will detect a person 11 km away on a clear night with no moon (starlight conditions in the industry jargon) have been purchased by Iran to be deployed along a border. Towers 175 metres tall with the cameras on top will be erected every 21 km, according to Brad Ganther of Lenzar Optics.

The unit is apparently the most sensitive commercially available low light level system. It incorporates a new lens from Lenzar, the only U.S. TV lens maker and an ISIT (Intensifier Silicon Intensifier Target) TV camera from Impossible Electronic Techniques. Both firms were exhibiting last week at an exhibition of security systems and equipment at the U.S. Trade Centre, London.

Under starlight conditions, the system is actually good enough to permit the recognition of faces of people 3 km away, Ganther said. During tests in Florida, the unit has apparently been used to watch people in flats several km away.

Because low light level systems simply intensify existing light, they are seriously affected by weather. Rain, fog, or even a heavy cloud can cut the range in half.

Thus the U.S. Army opted instead for infrared cameras, which respond to the natural heat of people or tanks and can see at all times. Ganther is highly critical of this choice, arguing that infrared gives poorer images, has a maximum range less than half his new unit, has

substantial maintenance problems because it requires a cooling unit, and is 10 times more expensive.

The new lens-camera systems cost $42,000 (£17,000) each, dropping to half that in quantity. The lenses have automatic internal filters and irises so that they can be used continuously day and night. The ISIT camera uses two fibre optic intensifiers coupled to the faceplate of a silicon target vidicon.

Ganther admits the only possible users for the new system are "people who want to kill each other", which makes the unit highly political. He said that the U.S. State Department would not permit him to ship the lens to a security show in the USSR last year. He also alleges that the State Department official who interviewed him had copies of all telegrams between him and the Soviet conference organisers.

[From New Scientist, June 12, 1975]

Machines Dial 999 and Talk to Police

No longer do burglar alarms simply ring a bell. Now they dial the police directly with a taped message, then ring company officials. In the U.S. there are possibly a million of the units in use, while in the UK there are tens of thousands.

But 98 percent of the calls are false alarms, according to studies in Britain and the U.S. And the machines have no way of knowing if they have been connected to the correct party and if anyone is listening. Most machines repeat the same message continuously for five minutes. Others dial each number twice in case the first try was misdirected.

Police in many U.S. cities have become so unhappy with the false alarm problem that they are prohibiting the machines from dialing the police and insisting instead that they ring a security service or telephone answering service.

When Los Angeles police imposed their rule two years ago, they cited the case of a petrol station dialling machine which rang them 67 times in 36 hours, according to Dr. Richard Bettinger, president of Betco Electronics, at the U.S. Trade Centre security exhibit last week.

But in Britain, the police are encouraging the use of automatic diallers, known as "999 units" in the UK because they commonly dial 999 with a police approved message. Generally the units replace alarm bells directly wired to the police station. As leased lines are becoming very expensive, users prefer to switch to diallers.

The British police seem willing to accept the false alarm rate because they want to encourage the use of the 999 system, and because the tapes can provide more information than a light on a board can. Many police forces, however, contact people whose alarms have a high false rate, and refuse to respond to the alarm if the problem is not corrected.

Meanwhile, the manufacturers work to correct the defects of the automatic diallers. Betco claims to have cut out 95 percent of the false alarms by adding a microphone on the site, which is automatically turned on after the taped message is finished. The operator, can then listen for thunder claps or other common causes of false alarms, as well as for footsteps and other indications of a genuine alarm.

[From New Scientist, June 19, 1975]

New Scientist 19 June 1975 647

Semiconductor scene

Packets of charge instead of currents

Though still a year or two off widescale application, the charge-coupled device (CCD) is emerging as one of the most versatile of integrated circuits since MOS technology first began. It is equally at home handling analogue as well as digital signals—promising a new computer memory, minute TV cameras and advanced radar processors

Roy Price
specialises in information retrieval and patent searching, and is the author of a major bibliography on CCDs

With all the spectacular advances in electronics recently, one thing the engineer has not had available is a single device which can handle both analogue and digital signals. Now the charge-coupled device (CCD), a development of the metal oxide semiconductor (MOS) technology already widely used, is emerging as a new kind of component which can perform both these functions. Combined with its small size and potentially low cost, this unique advantage is opening up a remarkable range of potential applications. A rival to the magnetic disc for computer memories, a solid-state imaging device to allow matchbox-sized TV cameras, a sophisticated signal processing component in advanced military radars, or night sights—these are just a few of the ideas beginning to move out of the laboratory and into real life application.

The CCD can perform this feat equally digital or analogue because its operation depends on the transfer of packets of charge rather than values of current or voltage. If the device chooses to count the discrete packets then its operation is digital, if instead, it looks at the total value of the charge then it is analogue. The charge can be introduced into the device electrically—for example, as a binary data stream—or be generated as a pattern on the surface of a light sensitive silicon imaging device. The versatility of the CCD is beginning to suggest wholly new concepts in system design to engineers all round the world.

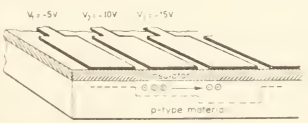


Figure 1 In basic three-phase CCD, V_3 electrode creates deepest potential well in which electrons are stored. Voltage on the following electrodes are manipulated so that the deepest potential well is moved under all V_1 electrodes, then V_2 and so on

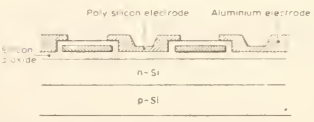


Figure 2 In the "buried channel" device, charge transfer and storage takes place in the n-type layer. By controlling the thickness and impurity concentration in this layer the device may operate in the 100 MHz region. The electrode construction shown protects the critical inter-electrode areas from ambient effects

The first CCD, made by Willard Boyle and George Smith at Bell Laboratories, was simply an array of closely spaced electrodes on a layer of silicon dioxide insulator covering a silicon chip. If a voltage was applied to the electrode, the region beneath it in the silicon became depleted of carriers, creating a potential well. A packet of charge could be stored in this region, at the interface between the silicon and the insulator. Then, by varying the voltage on the electrode, the depth of the well could be changed. And if the electrodes were spaced close enough, the charge could be transferred from one to another by tipping it from one potential well into a deeper one next door. The elements of a functioning device began to come together.

In Boyle and Smith's device, three electrodes were required to store and transfer one packet of charge. A series of these electrodes, with every third one coupled to the same clock line, forms a three phase shift register (see Figure 1). Every time the electrodes are clocked, the pattern of charge packets in the register shifts a stage so it can be used as an analogue delay line—with the time delay depending on the clocking rate and the number of stages. Needless to say, life is not quite so simple—and one of the first problems encountered was poor charge transfer efficiency. Michael Tompsett, an English expatriate working at Bell Labs, recalls that on dry days their early CCDs would not work without being breathed on—preferably with alcohol tainted breath.

The problem is that the complete charge packet is not transferred cleanly from electrode to electrode. In practice a small fraction of the charge is left behind temporarily, the result being that the original clearly defined packet gradually gets smeared out. In a long shift-register this can render the signal meaningless. Many solutions have been proposed to improve charge transfer efficiency—as many as the number of workers in the field, according to some cynics.

Two of the most important are the "fat zero" and "buried channel" techniques. Fat

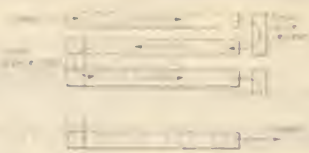


Figure 3 The operation of a charge-coupled device

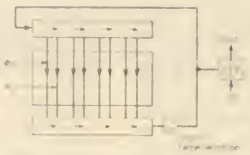


Figure 4

Figure 4

Critical trade-off

Random access

manufacturing side first; the present chip is vast by semiconductor standards -half an inch by three-quarters of an inch—and would be far too expensive for the consumer market

The basic principle of this and other CCD imagers is that light from the scene being viewed is focussed on to the surface of the silicon chip, where it produces a pattern of charge, using in some cases MOS devices which are photosensitive. Then the charge can be read out using CCD techniques. But, again, the detailed organisation of the device is vitally important to its performance and economics. Two broad options for organising these imaging devices have been proposed —frame transfer (FT) and interline transfer (ILT).

The frame transfer organisation is functionally simplest, consisting of an imaging area, a temporary storage area and an output register (see Figure 5). The image is allowed to build up in the imaging area and then clocked out into the storage area, shielded from the light, while the next image builds up. Then the signal is read out serially through the output register. Interlacing—the technique whereby a television picture is created from two alternate frames of interlacing lines—is possible by this technique, but it is difficult to get good vertical resolution.

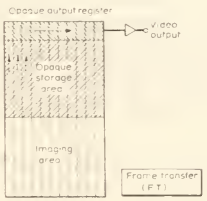


Figure 5 The "frame transfer" structure is used in a camera with TV resolution, although it requires a large silicon area

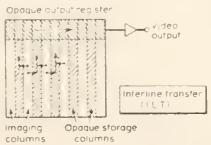


Figure 6 Interlacing may simply be achieved in "interline transfer" by transferring the signal from the imaging columns alternatively into left-hand and right-hand storage columns. With a sensitive amplifier, this form of organisation can detect the equivalent of 30 electrons

Fairchild is one of the companies which has produced devices using a variation on the interline transfer technique (see Figure 6). One example is an imaging device where 190 columns each including 240 photosensitive sites alternate with 190 CCD shift registers. The signal built up in the photosensitive sites is clocked out to either the left hand or the right hand shift register, and then read out, line by line. This type of device is ideally suited to interlacing, and makes an efficient use of silicon area. By using buried channel technology with high transfer efficiency, it can be used as an imager in low light level applications—perhaps in military and security equipment.

Processing analogue signals

A third major application area for CCDs—and perhaps the biggest—is in analogue signal processing. The scope here has received less attention because much of the work is on defence development contracts and masked by military security. Increasingly, engineers have been tackling the problem of filtering input signals—for example, from radar echoes —by digital techniques. This usually requires expensive analogue-to-digital conversion units, which digitise the incoming analogue signal for processing. On the other hand, analogue techniques are still preferred where the number of filters needed is small and the stability problems are not too great.

CCDs can combine the best features of both the analogue and the digital approaches—at a low cost. In one case, quoted by Dennis Buss of Texas Instruments, a complex filter which would cost $4000 and dissipate 45 watts in its digital version could be built for $66 and dissipate only 0.6 watt if it was made with CCDs.

The simplest example of the virtues of the CCD is the analog delay line, quoted earlier. For example, every PAL colour television receiver includes a 64 microsecond delay line as part of its colour circuitry; the role could well be taken over by CCD eventually. Beam forming in sonar and seismic data processing is achieved by delaying the outputs of the acoustic transducers by differing amounts; every moving target radar needs a programmable delay line of some kind to compare successive images; a variable delay can be used to iron out speed variations in video or audio tape playback speeds. Already one commercially available tape recorder allows dictation and replay at different speeds without voice distortion by using a form of CCD.

Thus, in many different areas of technology, CCDs are on the threshold of important applications—yet they are still very much in the development phase. Controversy still rages over the best ways of achieving high charge transfer efficiency and the most appropriate chip organisation for different functions. Commercial devices are announced with increasing frequency, but very few customers are putting them into standard products as yet. This is a situation which must change dramatically in the next year or two. The advantages of CCDs are becoming too strong to ignore.

[From New Scientist, July 3, 1975]

Big Brother Watches Orly Passengers

Visitors to Paris might be surprised to learn that as they pass through the immigration check at Orly Airport, they are being scrutinised by a Ministry of Interior computer. With a newly-introduced computer system, police at Orly can check their records in less than 30 seconds.

Previously each passenger through Orly filled in a card and handed it to the authorities with his passport. If the policeman had any suspicions about the passenger, he placed the card on a conveyor belt which took it to a filing section. A clerk checked the card against the files and if the passenger was on the wanted list passed this information to the policeman upstairs. Meanwhile, the passenger was wending his way through the remaining formalities—holding him while the card was checked would have taken too long. The police did not always succeed in catching wanted persons before they fled the scene.

The computer system speeds up the whole operation. The front line policeman places the card on what looks like a photocopier. This transmits a picture of the card to three operators in another room. They type into the computer system the passenger's name, age, and nationality. These data are transmitted to the Ministry of the Interior itself. Within 10 seconds the airport terminal displays either "positive" or "negative".

Negative means that the passenger is harmless and can be allowed through. However, if the response is positive, the police have to take action. The system may indicate "hold", in which case the operator presses a red button and the passenger is held by the police. Or it may show "watch", indicating that the customs officer should thoroughly search the passenger. The whole operation, from handing in the card to issuing instructions to the police, takes 30 seconds.

Commissioner Roux, responsible for the operation of the system, says that there is still a human element. Even a hold-up as short as 30 seconds for each passenger would lead to bottle-necks, so not all passengers are scrutinised. "But," says Roux, "we are nearer to getting our hands on people we would like to interview."

[From New Scientist, July 10, 1975]

New Scientist 10 July 1975

Boardroom electronic warfare

As bugs become more sophisticated, so do the electronic countermeasures, in an escalating warfare that has led some electronic poachers to see more profit in gamekeeping

Dr Joseph Hanlon

The latest addition to the bugging arsenal is a device which will broadcast continuously for a year, but is no larger than a matchbox. No longer will the bugger have to link his device to the mains, or sneak back repeatedly to change batteries. The new device, according to developer J. J. Griessen of Technique Sécurite Développement, Geneva, is powerful enough to be heard 150 metres away.

Matchbox size is a bit large, and one of the big sellers (2000 sold at £350 each, Griessen said) is a 15x11x5 mm bug—small enough to sit on a fingernail—which will also broadcast to a listener 150 m away. But power is the problem—its life is only 25 hours. A half size unit is available for £400. It is only 14x5x4 mm, but its life is limited to 4 hours. And Griessen is about to sell a smaller unit (see photo).

Such devices can easily be hidden behind curtains or under a desk by someone sneaking into an office or conference room. For a good signal, they need an antenna, which can be easily hidden as well.

One solution to the power supply is to let the victim provide his own. Lee Tracey of Technical Security Ltd., London, claims to have put a bug into a pocket calculator which was to be given to the person to be bugged. It was intended that the victim would generously take the bug into meetings with him and supply the power by replacing the calculator batteries whenever needed. Such a bug would draw too much power if left on all the time, so Tracy said that it was radio controlled—to be turned on or off at will.

On the other end of the spectrum, effective and small bugs can be purchased by post through advertisements in magazines such as Wireless World for as little as £7·81. In one recent advert "the smallest transmitter available in the UK which can be "held in the hand or operated in a drawer' was offered for £15·50, with a receiver for £13·25 if required. Cheap broad band receivers now available permit bugs to work outside the normal FM band. And devices like baby minders—mains intercomms with a small microphone to be placed in the baby's bedroom and a speaker for the parents' room—make excellent bugs.

EMI's Bughound in use at the conference table. Devices like this often must be brought within a few cm of a bug before it can be detected

Possibly the smallest bug commercially available is the most recent design from Technique Sécurité Développement, Geneva. This is only the microphone and transmitter; a miniature battery (perhaps half the size of the bug itself) and aerial must be added

Anti-bugging is big business

All this has made anti-bugging big business, with EMI joining the numerous small firms (many run by people better known for selling bugging devices) that now make bug detectors. The most common form of bug uses a radio transmitter, usually in the FM band (88-108 MHz). Most detectors aim at this type of bug, and work in a similar way: they incorporate a broad band receiver (usually 1 MHz to 1 GHz) and a field strength meter, and sound an alarm if the meter shows a signal above a predetermined background. Most commonly, the signal is proportional to the total field strength, so that a geiger-counter-like click goes faster or a tone gets louder as field strength becomes stronger.

Two hand held devices in this category are the EMI Bughound (£100) and the RFD-1 (£47) from Technical Security Ltd, London. Communications Control Corp of New York showed several units of this sort (£220-£400) at the US Trade Centre security exhibition in May.

These devices have two major problems—weak bugs and spurious signals. Sensitivity must be kept very low in urban areas with a substantial radio background, which means that the detector must be brought within 1-2 metres of an average bug, and 1-2 cm of the weakest bug. Often the detector aerial must be in the same plane as the bug aerial. In practice the devices will miss weak bugs, which must be found by a detailed physical search of the room. These detectors are also ineffective against bugs turned on by remote control or brought into a room after a meeting

starts. Even if the detector is left turned on and sitting on the conference table, the detection range is less than a quarter of the pickup range of a typical bug, so a bug could simply be brought in and left near the door.

As well as missing some bugs, these detectors pick up spurious signals—and there is no way to tell if a signal comes from a real bug. Derek Ainsworth of EMI admitted that "a taxi 100 yards away can give a signal on the Bughound". Perhaps the most serious problem is standing waves, which can build up from ordinary radio background to give very strong signals in enclosed metal areas, such as radiators, electrical junction boxes, and ventilation ducts. Ainsworth noted that in an office near the BBC, he picked up a very strong signal from an electric conduit—and it turned out to be Radio 2. Lee Tracey of Technical Security admitted (perhaps because he is about to sell a more sophisticated device) that 20 feet of ducting was torn out of a Greek government building based on a signal received on his RFD-1 that turned out to be only a standing wave. Ainsworth also noted that badly wired chandeliers give off relatively strong radio signals.

Looking for feedback

The next step, then, is a device which is both more sensitive and will indicate if a signal is really a bug. Technical Security is about to market its Scanlock (£940) to do this. It automatically sweeps from 10 MHz to 4 GHz, then locks on the strongest signal.

Scanlock has four operating modes. In the "audio" modes, it will demodulate AM or FM signals and simply act as a radio receiver. This immediately picks out taxi radios, the BBC, etc. It also shows up very powerful bugs, because they pick up the signal and rapidly build up an ear splitting feedback.

To show if weaker bugs are in use, there is a "soundwave" mode in which Scanlock broadcasts a tone and then looks for that tone in the strongest radio signal, sounding an alarm if it finds it. This feature permits the elimination of false alarms due to taxi radios and standing waves. But Tracey admits that this will only work for AM or FM bugs, and not for other modulations or codings. The device is portable, and is intended to be carried around in this mode to look for weak bugs.

In a demonstration in Tracey's office last month both Scanlock and RFD-1 were used against a weak transmitter concealed in a pen. The bug was good enough to pick up voices anywhere in the room and transmit them at least 20 metres, sufficient to be picked up in a nearby room or a car parked just outside the building. RFD-1 had to come within 2 cm of the device, while Scanlock picked it up about 2 metres away.

The significantly greater sensitivity of Scanlock makes it usable to check for bugs which are brought into a room or turned on by remote control. The sensitivity is adjusted so that the device just rejects all normal background signals, and the device is put into "soundwave" mode. The tone is sounded only if it receives a signal above the background, and the alarm will sound only if the tone is fed back through a bug and not if the signal is from a transmitter outside the area.

If there is still a serious fear of very weak transmitters—which are quite adequate to send signals, say, to an adjoining hotel room—the only choice is a device which requires an operator and which looks separately at each radio signal being broadcast, rather than just the strongest.

J. Donne Huldings, London, sells a hand-

Few barriers to bugging

Ownership and sale of bugs and wiretaps is legal. In certain circumstances, the manufacture and use of such devices may also be legal.

"There is little in either the civil or criminal law to control technical surveillance devices" in the UK, warned the Younger Committee on Privacy three years ago.

Last November the House of Lords reduced even that protection by eliminating one of the offences normally used by the police against privacy invasion. The Lords ruled that the crime of conspiracy to effect a public mischief does not exist. The decision came in an appeal by the Withers brothers, who had been convicted of that conspiracy for allegedly using bugging devices. The ruling came too late for the directors of Tracing Services Ltd., who pleaded guilty in 1969 to the same conspiracy charge after posing as government officials to obtain confidential information.

As information is not property, it is not an offence under the Theft Act 1968 to take information. The Law Commission further stressed the lack of protection last December when it warned that action for breach of confidence would not provide a remedy where the information had been obtained not, say, by breach of confidence by an employee, but by a bug.

There appear to be only three acts which relate to bugs: the Wireless Telegraphy Acts 1949 and 1967, and the Theft Act 1968. The Wireless Telegraphy Acts require a licence for all radio transmitters (such licences are almost never granted) and makes it illegal to listen to non-public broadcasts. There are about 80 prosecutions per year under these acts, primarily against pirate radios, but occasionally against people who use bugs.

The Theft Act 1968 has a provision on electricity which makes it an offence to "dishonestly use without due authority, or dishonestly cause to be wasted or diverted." This would make it an offence to use a bug which drew power from telephone or electricity lines (such as a mains bug). But if a bug had its own battery and was put on to the mains, could it be said that mains electricity was diverted into a new circuit without actually being used?

In any event a bug which has its own wires and power source appears to be completely legal so long as no damage is done to a building when the bug is installed!

Younger and the Law Commission both stressed that existing laws are ineffective, and both reports have been met by governmental lethargy. Now that the Lords have removed one of the few barriers to industrial or private espionage, the government must be persuaded to act. In the meantime it is best to heed the Law Commission's advice: if you want to protect confidential information, disclose it in confidence to a person whose surveillance you fear in order to ensure your right to a subsequent action for breach of confidence.

Patricia Hewitt
Secretary, National
Council for Civil Liberties

Buying bugs by post

Anyone can buy a bug by post. The Exchange and Mart last week (3 July) had two ads for VHF microtransmitters, one for a kit, and two for plans of how to build them.

The two advertisements shown are from Wireless World (April). We ordered the cheaper (up to £7.41 due to VAT increase), and two days later received our bug (above). It took only a few minutes to assemble (right).

But in putting it together, we violated the law. The Radiotelephonic Transmitters (Control of Manufacture and Importation) Order 1968 bans the "manufacture whether or not for sale" and the importation of [illegible] 29.7 MHz and 88 to 108 MHz range. The [illegible] from the US and Japan. The latter is [illegible] VHF (or FM) [illegible] used for bugging devices [illegible] avoids the [illegible]

In practice, the Home Office [illegible] not to prosecute people [illegible] devices so long as they make [illegible] the ad that the units are not [illegible] in the UK. The upper ad violates this policy and the Home Office reports that similar advertisements have been prosecuted under the Trade Descriptions Act.

held Illicit Transmitter Detector (£850) which covers 34 to 874MHz (Donne, like Technical Security, also sells bugs.) Diversified Corporate Services, London, sells the more elaborate A2 Miniature Surveillance Receiver (£4000) which has a visual display and covers 2kHz to 2 GHz.

Both units could clearly be used during meetings and are sensitive enough to pick up bugs brought in or turned on after the meeting starts. But they do require an operator to regularly sweep the radio bands.

Listening on the electrics

Radio transmitters are not the only way to bug a room. The alternative is to send the signal out over wires. Indeed, the only kind of bug that cannot be detected electronically is one where the listener installs his own wires, often hidden behind skirting boards, under carpets, etc. These can only be found by a physical search.

But rooms have mains electricity wires coming in already and offices have intercomms as well. It is easy to send a radio signal over the mains wire, and it can be picked up at any socket on the same side of a transformer—on another floor or even in another building. Plug-in wireless intercomms work this way, and mains bugs can be fed in easily directly in a socket or light switch. But any mains intercomm will also pick up the signal.

Diversified Corporate Services, London, sells a Bug Detection Unit for £250 that combines the simplest type of radio bug detector (similar to Bughound) with a low voltage test circuit for intercomms and a mains tester to look for a mains intercomm.

Clearly the increasing squeeze on corporate profits and rising political dissent has led to an escalation of electronic spying on corporate and political opponents, which in the West military tradition has led to an electronic counter-measures capability. Beating the buggers depends on how much you are willing to pay. Ainsworth argued that "the big danger area is not the sophisticated devices, but rather the cheap, self-manufactured bug planted quickly—the grudge thing on your employer thing." But where large profits are at stake or governments are frightened, even sophisticated devices will seem cheap.

Next week: The telephone tells all. Can a telephone be used to bug your room and how to find out if your phone is bugged.

How we bugged the Commons

New Scientist bugged an MP's office in the House of Commons with a radio transmitter so powerful that a staff member standing on Westminster Bridge was able to listen to the MP's conversations.

The whole exercise was much easier than we expected. As amateurs our success shows that anyone can bug an MP — or a corporation executive, competitors, their boss, or friends and neighbours with little difficulty. For a professional it would be trivial.

Miniaturised transistors really make the difference. No reasonable security system in the House of Commons or a large corporation can stop someone from bringing in a bug. Anyone who can find a reason for an appointment can leave a bug behind, a professional with just a minute or two alone in an office can plant a highly sophisticated device.

The "victim" in our case was Tom Torney, an MP known for his strong antibugging stand. Joseph Hanlon planted the bug on Tuesday, 1 July during an

New Scientist's bugging equipment. Standard FM radio receiver with the transmitter and batteries in front. In front of the transmitter are the aerial (left) and microphone (right)

McGinty and Hanlon enter the House

The bug was concealed in a jacket pocket

interview—about bugging. Two other New Scientist staff members listened in and taped the conversation. Enid Broderick on Westminster Bridge and Lawrence McGinty inside the House. Robin Corbett, another MP known for opposition to bugging, was in on the plan (though our experience shows that in most real bugging situations such inside help would not be necessary).

Our transmitter was little bigger than a cigarette packet. It was made by an electronics technician, but its construction required no special expertise and small transmitters—as well as plans and components—can easily be purchased. The receiver was simply a good quality FM radio, lent to us off the shelf by Laskys Radio, London.

To produce a signal that could be picked up far enough away the bug needed an aerial more than two feet long. So we concealed the aerial and a microphone in a briefcase. Cases are inspected at the St Stephens entrance to the House, so Hanlon carried the transmitter in his pocket until he reached the Central Lobby. There, he opened the case and plugged in the transmitter, with no one paying any attention.

Torney and Corbett met Hanlon and McGinty in the Central Lobby. Hanlon accompanied Torney to his office for the interview, Corbett took McGinty to another office to listen in. McGinty did not need Curbett's aid to do this—in a building such as the House with so much public access, it would be impossible to stop a determined person from wandering into private areas.

The quality of McGinty's tape was as good as if he had been in the office during the interview. The quality of Broderick's tape on the bridge was not so good—the signal was weak and there was a lot of radio static. Yet the tape was understandable. And when we had it cleaned up somewhat by Hugh Ford of HF Engineering, Sunbury-on-Thames using techniques available at any recording studio, the tape was easy to follow. The professional "bugger" would have both a much better receiver, reducing the noise, and access to these processing techniques.

Among the things we recorded were a telephone conversation in which Torney set up a meeting with a minister. (In fact, Hanlon was present during the call. We intentionally did not record anything that Hanlon was not actually present to hear.)

After the interview, Torney and Hanlon left the office, but Hanlon left his briefcase behind, still broadcasting. McGinty quickly packed up his radio and left too. They returned to the corridor outside the committee rooms (where the public is normally permitted).

In the corridor they explained to Torney that he had been bugged. Having said during the interview "I don't think there is any bugging in this building" Torney was clearly shaken. He and Corbett then agreed that the incident should be made public.

The problem is not security at the House. The devices are just too small to be found even by regular searches in a building visited by thousands of people every day. Any member of a delegation seeing an MP or a company head could leave such a device behind, or carry in a bugged briefcase. And a briefcase is so much a part of the office scene that—as in our experience—it probably will not be noticed even when left behind.

In a letter on 30 May to Robin Corbett, the leader of the House, Edward Short, said "I can assure you that rooms that are regarded as sensitive are swept [for bugging devices] from time to time." But neither those sweeps, nor reasonably tighter security would have stopped us—or any determined amateur or professional.

On Westminster Bridge, Enid Broderick listened

Tom Torney outside the House displays the bug

[From New Scientist, July 17, 1975]

The telephone tells all

Since the first operator listened in on the first telephone call, the telephone has been the most important instrument of electronic surveillance. Modern versions of the traditional tap remain undetectable. And the telephone can be used to listen in on room conversations, even while the phone is on the hook.

Joseph Hanlon

inductive tap is a coil placed in the field created by the current fluctuations during a telephone conversation and is often used by people to record their own conversations. In principle, the coil could be put anywhere near a telephone or telephone wire and is electrically undetectable, but its reception is good only in or on the telephone instrument itself. Thus it must have a radio transmitter, and can be picked up by a bug detector. The other method is the tap connected in series or parallel with the telephone, which uses the telephone current to operate a radio transmitter or tape recorder. This is believed to be the most common non-exchange tap, but it adds a resistance similar to an ordinary telephone, which halves the voltage passing through the subject's telephone, making it easily detectable.

Bugging the 'phone

It is with telephone connected bugs that the electronic warfare has reached its most sophisticated. Telephone connections are most desirable because the bug can be operated from far away, needs no external power source, uses the microphone already in the telephone (which itself is already placed in an optimum location in the room), and uses existing wiring. The problem is that the bugs must be difficult to detect and must permit the subject to use this telephone normally.

With one exception (the infinity transmitter), the listener must tie into the line somewhere between the subject's telephone and the central exchange. There are usually two or more terminal boxes where this can be done easily: the box inside the building where all the lines from the office are brought together, to tie into the Post Office cable, and the green box along the road where many Post Office cables come together.

These boxes are already a jumble of wires, and a few more will be unnoticeable. The "bugger" who knows what he is doing can easily open the box, find the correct wires, and make his connection without anyone realising he is not a Post Office engineer. The link can be a direct wire (sometimes using a spare Post Office line), a radio transmitter placed safely away from the room being bugged and thus beyond the reach of bug detectors, or a tape recorder. Connections can also be made by cutting into the telephone wire, and links can be made at the central exchange, either with or without the knowledge of the Post Office.

The simplest telephone bug is the direct connection, in which a new microphone is installed in the telephone in parallel with the ringer and the handset. Indeed, the ringer itself contains all the components needed for a microphone and it sometimes acts that way (its microphonic quality is poor, but can be improved). Direct connections can be designed not to interfere with telephone conversations, but can be detected simply by listening on the line with the receiver on the hook.

More sophisticated telephone bugs are the hookswitch by-passes—special attachments which make the telephone appear off the hook to the listener but not to the exchange. A simple capacitor will by-pass the hookswitch, blocking the d.c. voltage from the exchange but passing the audio a.c. This uses the dynamic earphone as a microphone, and has poor sound quality. A 10 000 ohm resistor will pass enough current to activate the carbon microphone in the handset but not to activate the exchange, but this, too, provides a poor signal. Putting a resistor and capacitor in parallel, however, provides a very good signal and does not interfere with normal telephone calls.

These devices operate at all times, and can thus be detected by listening to the line while the telephone is on the hook, as well as by measuring current flow (no current should flow when the telephone is on the hook, while the resistor clearly will pass a small current).

Next in sophistication are four hookswitch by-passes which can be turned on by a signal from the listening post, preventing its detection simply by listening on the line. Usually, these involve cutting the phone off from the exchange line, so provision must be made to restore instantly that connection and cut off the by-pass if there is an incoming call or the handset is lifted for an outgoing call. Automatic switches exist to do this.

The first technique is a reverse biased diode, which closes if the normal telephone line polarity is reversed. This can, of course, be detected by reversing the polarity and listening.

A neon lamp requires about 65 volts d.c. to fire but then conducts like a closed switch. Since exchange voltage never exceeds 50, it remains an open circuit until the listener adds the extra power. Up to seven lamps can be put in series to increase the breakdown voltage to escape detection. But current must be limited, so the signal is noisy. A zenor diode, however, has a similar voltage breakdown characteristic and will conduct much more current, providing good signals.

Most sophisticated of all is the four layer by-pass, such as a triac, which requires a microsecond high voltage pulse to turn on, but then remains closed with the minimum current flow. Firing voltage can be up to the breakdown level of the telephone itself—over 3000 volts—making them difficult to detect. These devices are available on chips 2 mm x 2 mm x 0·1 mm which are easily concealed in the telephone.

Listening a continent away

Finally, there is the one hookswitch by-pass which does not require a listening post connected between the telephone and the exchange. The infinity transmitter uses a tone activated hookswitch by-pass and can be listened to anywhere in the world. The eavesdropper rings the subject, apologises for a wrong number, and then keeps the line open by not hanging up when the subject hangs up. The eavesdropper then sounds a tone, which activates a hookswitch by-pass, making the telephone act as if it were off the hook again. The trouble is that the line is blocked to incoming calls, and in Britain can be defeated simply by picking up the phone after every

Is telephone tapping legal?

"Parliament may wish to consider whether legislation should be passed to render the unauthorised tapping of a telephone line an offence," suggested the Committee of Privy Councillors appointed to inquire into the interception of communications, in its 1957 report (Cmnd 283).

Apparently Parliament did not wish to consider such legislation, and thus there seem to be a wide range of circumstances in which one can legally tap a telephone.

Curiously, while the Post Office (Protection) Act 1884 makes it an offence for anyone to forge or alter a telegram, the Act only makes it an offence for a "person being in the employment of a telegraph company" to divulge the content of a telegram. This law now also applies to telephone conversations, and thus only official tapping seems covered by it.

Until 1937, the Post Office intercepted telephone messages without warrants. But then the Postmaster General and the Home Secretary decided that this was "undesirable" and they agreed to apply the procedure—dating back to at least 1663—for intercepting letters only with warrants from the Secretary of State. The Privy Councillors Committee reported the number of telephone taps from 1937 to 1956. The number peaked at 180 in 1941, but fell to 66 by 1945. After that it rose steadily, averaging more than 200 per year in 1953-6. No statistics have been released since then, but the number is widely thought to be substantially more now, and the Post Office has special telephone tapping circuitry available to be installed when needed.

Private tapping appears to be covered only by two sets of laws. Naturally, it is an offence to damage telephone equipment. But more relevant is the Theft Act 1968 provisions on electricity which makes it an offence to "dishonestly use [electricity] without due authority, or dishonestly cause [electricity] to be wasted or diverted." (This provision is not affected by a ruling last week by Lord Chief Justice Widgery that electricity is not property capable of being stolen. In effect, he said that misuse of electricity must be charged under this section and not as a more serious offence such as burglary.)

Clearly then, any tap which draws power from the telephone lines (the simplest taps do) is illegal. But what happens if the tapper does not damage the telephone when he installs his connections (which is not hard to do) and supplies his own power, perhaps to make the tap less detectable to the victim? He has added a new circuit to the system and thus the electricity may follow a new path—has he "diverted" the electricity even if he does not use any?

The same considerations apply to bugs which use telephone lines. Any which draw power from the telephone line must be illegal. But what about those which involve a hook-switch bypass and temporarily disconnect the telephone from the exchange, reconnecting it and disconnecting the bypass for any incoming or outgoing call? In this case it seems the electricity is not even diverted, except perhaps to signal the eavesdropper that a call is coming in.

With an infinity transmitter, the person doing the bugging actually pays for the call, so he cannot be said to be misusing electricity. But the hook-switch bypass is a different route for the electricity, and thus may be a "diversion."

Nevertheless, theft or diversion of electricity seems a minor offence compared to the seriousness of telephone tapping itself—and it may not always apply. *Joseph Hanlon*

incoming wrong number to force the eavesdropper to hang up. In the US, however, where telephone signalling is different, the eavesdropper can prevent the subject's phone from ringing and make the connection without him knowing.

The infinity transmitter is detected simply by a tone generator sweeping through the known range of triggers for the device, and listening on the line with the phone on the hook to see if room noise suddenly comes through. But just in the last year, two British efforts to beat this detection have come to light. The first is simply a modification which requires that the tone be sounded for three seconds, charging a capacitor, before the circuit closes. Tone sweeps will pass through the trigger tone much too quickly to have an effect. And Lee Tracey of Technical Security Ltd, London, has his own experimental improvement, which requires two tones to be alternated at a rate that has been previously determined.

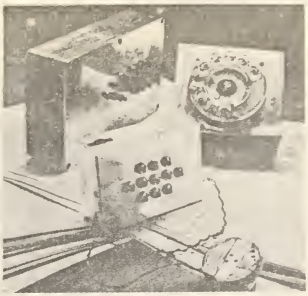
Bug and tap hunting

By far the most sophisticated telephone tap and bug detector now available is the Dektor telephone analyser (£2200). With the telephone on the hook it measures voltage (which should be 45-50) and current (should be 0) and permits the operator to listen for any signal being transmitted over the line, both before and after a tone sweep. The latter turns on infinity transmitters. For £200-£1400 Dektor sells a polytonic sweep attachment which, according to Dektor head Alan Bell, triggers two-tone infinity transmitters (Tracey disagrees).

Next, voltage and current are measured with the telephone off the hook. Finally, with the telephone disconnected from the exchange, resistance and capacitance are measured and an attempt is made to set up normal voltage triggered devices. If any of these shows up, a special oscilloscope shows a pattern identifying the type of device. Finally, if no bugs have been found, a short 6000 volt pulse is used to trigger four-layer devices.

A simple device for testing telephone lines is manufactured by Communications Control Corp, New York (£1400-£2600). This device does the on- and off-hook voltage test, on-hook listen, and tone sweep. But to check for other hook switch by-passes, a capacitor is charged to 1000 volts and permitted to discharge for three seconds. Normal leakage in the system should not permit it to drop below 600 volts in that time, but any by-pass will provide a much more rapid leakage path. This ingenious device should find any extra connection in a telephone instrument except a four-layer device triggered by more than 1000 volts. But it may be less effective for devices on the telephone line.

Dektor also sells (£1500) a permanently installed bug and tap detector called the Cloak of C.I. Linked to the telephone and mains, it provides a series of regular automatic tests. First, it automatically sounds an alarm if the electrical characteristics of the telephone go out side the normal range—thus showing



Phone phreaking equipment, including an old-style AC9 simulator (rear right) and its present push-button equivalent (front right) which includes a telephone earpiece as its acoustic coupler. The touch-tone, or multi-frequency, simulator (rear left) is a unit used largely in the United States. Beneath the three pieces of equipment is a copy of the Post Office's own telephone codes

up hookswitch by-passes as soon as they are turned on and extension telephones when they are picked up. Next, it has a simple feedback bug detector, which sounds a tone and sweeps the radio spectrum (from 0·1 to 100 MHz), the telephone line itself, and the mains for just that tone, sounding an alarm if it is found. The device is set automatically to sound the tone and do a quick bug check every time the telephone rings, thus adding its objectionable noise only when the user of the room has already been disturbed. This device should pick up most bugs and taps, but will miss relatively low powered and high impedance taps.

All of these devices will have some trouble with the vagaries of the electrical characteristics of the telephone system, and it is useful to build up a record of normal voltage, current, and network resistance. But if this is not available, standards can be set by comparing with other telephones in the office. But all of the electrical characteristics can vary dramatically over time. Impedance, for example, varies from phone to phone, depending on line length and other characteristics; rain can totally and suddenly change the electrical properties.

Both firms have interesting backgrounds. Dektor sells the Psychological Stress Evaluator, a lie detector which is supposed to operate by looking for stress in the voice (see New Scientist, vol 62, p 219). Dektor's head, Alan Bell was responsible for the report that the famous Nixon tapes were not doctored, a contention thrown out by the official experts (see New Scientist, vol 50, p 738). Ben Jamil, who demonstrated the Communications Control equipment at the US Trade Center show, spent more than 10 years selling bugging devices. His open sales of the devices through mail order catalogues and a shop in mid-town Manhattan were a major factor in the 1968 US law prohibiting the sale of such devices.

Preventing taps

The alternative to detecting taps is preventing them. Jamil sells a Wiretap Trap which can be attached to a telephone or purchased already built into a telephone designed to look like an antique French phone. The claims in his literature that it is a "virtually tap-proof telephone" and that it "knocks out any telephone operated room bugs" are clearly nonsense; even Jamil admits that it will not pick up many high impedance taps or hook switch by-pass bugs. But the device does prevent against series taps (by doing voltage checks) and many recording devices.

The last is the most significant, because the image of the bored eavesdropper with headphones is rarely true. More commonly, taps are monitored by tape recorders which are turned on only when the telephone is actually used. Virtually all such recorders are turned on by the drop in voltage on the line (from 50 to 10 volts) when the telephone is picked up. So the Wiretap Trap simply raises the voltage so that such devices are not activated. Such a device should be highly effective in beating most non-exchange taps.

But the Wiretap Trap fails to stop two other kinds of tape recorders—the less common voice actuated devices (such as Nixon used to bug his own office) and those on British exchange taps. In British exchanges, as distinct from US ones, there is an additional wire called the p-wire, which is earthed whenever a line is in use. It triggers ringing signals and dial tones and engages lines. (The reason that infinity transmitters cannot be used in Britain without the subject picking up the telephone is that here the only link between caller and recipient is the p-wire until the recipient actually picks up the phone.) Recorders on exchange taps in Britain are triggered by the control circuits being earthed, and this is not affected by increasing the line voltage.

Phone phreaks?

The Wiretap Trap bears a striking resemblance to the phone phreaks' black box, which is attached to a telephone and permits people to make calls *to* that telephone without being charged. Relays at the telephone exchange are triggered by current on the telephone line. Thus, if the voltage on the Wiretap Trap were set at 50, no current would ever flow and the exchange would never know a person had picked up the phone. The voltage is set at the highest level which still permits enough current to pass to trigger the relay giving a caller a dial tone. Each Post Office relay is triggered by a different current, however. Two other relays are involved in incoming calls. When a person picks up a telephone after it rings, the current moving in the completed circuit triggers first the F relay, which stops the ringing and links the caller and recipient together, and then the D relay, which sends a signal to the caller's exchange to start charging for the call. The dial tone relay requires the most current, than the D. The F requires the least. A black box simply uses a battery to provide enough voltage to keep the current above that needed by the F and below that needed by the D. Thus, the Wiretap Trap set in its normal mode to obtain a dial tone will not affect the exchange, but it could be used as a black box simply by increasing the voltage the required amount before an incoming call is answered.

[From New Scientist, July 31, 1975]

World's biggest chip makes tiniest TV camera

Using what is claimed to be the world's largest integrated circuit, researchers at Bell Labs in Murray Hill, New Jersey, have built a miniature television camera that gives the full resolution of broadcast TV. Other US manufacturers, including General Electric, RCA and Fairchild, have demonstrated miniature solid-state TV cameras but none so far claims to have achieved the Bell instrument's picture quality. Commercial TV resolution in the US is 525 lines, against Europe's PAL standard of 625 lines.

The experimental camera, measuring about $6\frac{1}{2}$ cm square by 15 cm long, is the latest in a series of solid-state TV cameras built by Bell Labs around a charge-coupled device (CCD) chip for potential use in a video-telephone system. Indeed, the charge-coupled device itself was originally invented by Bell, back in 1969, as an imaging sensor for its so-called Picturephone. Today, CCDs have found other important applications, including memory units that now rival even computer disc stores in price, performance terms, and versatile signal processors with a unique ability to work equally in digital or analog form (see *New Scientist*, vol 66, p 647).

The actual CCD chip used in Bell's latest camera measures no less than 16 mm by 20 mm and contains some quarter million sensing elements—equivalent in size, says Bell, to about 20 standard MOS chips used in pocket calculators. Its imaging region, a little over half the total silicon area, is equivalent to that scanned in a standard one-inch diameter vidicon tube used in conventional TV cameras. Its surface has 496 vertical interlaced scan lines and 475 horizontal picture elements engraved by an important new electron beam exposure system (about which the laboratory steadfastly refuses to release details).

World's largest integrated circuit was developed specifically by Bell Laboratories, New Jersey, for their broadcast quality TV camera

Tiny TV camera built at General Electric Research and Development Center, New York, weighs only one pound and is sensitive enough to take high quality pictures using the light of only one candle

While the CCD imager does not need the high voltage (one camera works off a small rechargeable battery pack) nor the electron beam deflection circuitry and vacuum envelope of the conventional camera tube, all the experimental cameras built by Bell so far still have inherent video faults. Blemishes appear on the screen as a result of defects in the readout from the shielded half of chip where the previous "scan" from the imaging section is held for readout to the TV monitor. The blemishes show up on the screen much like the spot faults inherent in all but the most expensive silicon vidicons. These can be tolerated in, say, low grade TV cameras for surveillance work. But to eliminate all blemishes from a CCD imager for a broadcast quality picture would demand the utmost cleanliness during the processing of the chip itself. This, in turn, would require a clean room facility at least one order of magnitude better than even the best facilities currently used for fabricating MOS integrated circuits. And achieving a useful production yield of such high quality CCD imagers could take years and many millions of dollars.

By contrast, in the imaging technique developed at General Electric Research and Development Center, Schenectady, the packets of charge are not transferred from cell to cell until they reach a readout line as in a CCD; instead, each pair of light-recording capacitors on the chip is individually addressed by scanning circuits, which cause the charge to be released by "injecting" it into the base of the chip. Such a charge injection device (CID) allows almost the entire chip area to be made photosensitive—which means that the device uses its silicon much more efficiently and consequently can be used to make a particularly sensitive camera. Indeed, one TV camera built recently by GE, weighing one pound and said to be the world's most sensitive, can even take pictures by candlelight (see photo). The product is soon to be launched on the security equipment market.

Though it has not yet got broadcast TV resolution, perhaps the GE camera's biggest potential advantage is that it does not have the in-built "dark current" problem of the CCD-based TV cameras. If a pair of capacitors in the chip fails, the result as in Bell's camera is a dark spot blemish on the screen. But because the charge in a CID is not passed from capacitor to capacitor for processing, there is no accumulation of errors across and down the screen—which, in a CCD camera, gives rise to a darkening effect that increases progressively towards one corner of the screen.

[From New Scientist, July 31, 1975]

Fluorescence Fingerprints Exploded Explosives

(By Adrian Hope)

In a string of three recent patents, Westinghouse Electric Corporation of Pittsburgh, Pennsylvania, claims a system of applying indelible identification marks to explosives. The aim is to enable manufacturers of explosives to label their products—not only with chemical identification but also with date of manufacture. Most important of all, the label information will be available even after detonation.

A small proportion of fluorescent conglomerate is mixed with the explosive material, with each individual conglomerate containing at least two different types of fluorescent material—a "spotting phosphor" and a "coding material". The spotting phosphors are of the type found in domestic fluorescent lamps and produce a wide band of emission when illuminated by ultraviolet light. The coding materials are of the lanthanide series of rare earth metals, and produce characteristic multiple line emissions when similarly illuminated.

It is claimed that, even after an explosion, there will be sufficient whole conglomerates in the area to enable positive identification of the explosive and its source. As the first stage of detection, the area around the explosion would be examined under conditions of darkness with an ultraviolet light. The spotting phosphors in any conglomerates present would emit visible light and could thus easily be picked up with a pair of tweezers. The collected samples would then be analysed with a conventional monochromator. The line emissions produced for a given illumination wave-length would be logged and compared with identification charts made available by the original manufacturer.

For the scheme to work and enable police forces around the world to identify the exact source of any explosives used illegally, it would be necessary for all manufacturers to incorporate conglomerates in their explosives and issue identifying information. The scheme would thus inevitably cost money to operate, but it would immediately curb the illegal trafficking of explosives.

[From the Washington Post, Apr. 21, 1975]

Laser 'Bug' in Nixon Office Reported

(By Austin Scott)

Penthouse Magazine said yesterday that President Nixon's Oval Office was secretly bugged before August, 1970, by a sophisticated laser beam transmitter hidden in the wall and concealed beneath a coat of fresh paint.

In an article written for the July issue of Penthouse, former foreign correspondent Tad Szulc said the device was "apparently controlled by one of the (U.S.) intelligence agencies," and, unlike a tape system, could identify every individual voice in the room as well as separate several simultaneous conversations.

William Hawthorne, a Secret Service spokesman, said when asked for comment that the Secret Service knows of no such bugging and does not believe such a device was ever installed.

The article said the transmitter was removed in August, 1970, and that one or more senior officials of the Secret Service and the Central Intelligence Agency knew of its existence.

Szulc said the purpose of the transmitter, the identity of those who ordered it installed, whether the Secret Service and the CIA officials knew about it before it was removed, and whether Nixon ever knew about it are unknown.

Hawthorne said he had checked with the Secret Service officials responsible for the Oval Office at the time in question, and that they were not aware of any such device.

"We don't believe it could have been installed," Hawthorne said.

Szulc said the laser beam bugging operation went by the code name "Easy Chair."

"Highly authoritative sources" said the bug was installed by a foreign-born painter employed by the government, Szulc wrote. He said he knows the name of the painter, but withheld it from publication "to avoid causing suffering and embarrassment to persons innocently involved in this operation."

Szulc said only about a dozen past and present officials of the intelligence community know about "Easy Chair."

He said the laser bug picked up all telephone conversations, including those made over "secure" scrambler lines, as well as every conversation between Nixon and his aides, friends and visitors.

How far the transmitter could broadcast the pickups was not clear, Szulc said, but he said experts believe it probably had a transmission range of about a half-mile, so that the conversations could have been received anywhere in the White House, the adjoining Executive Office Building, the Treasury Building a block away, or even the Commerce Department three blocks away.

[From Penthouse Magazine, July 1975]

The Spy Among Us

The Constitutional Right of All Citizens To Be Secure in Their Houses Is Violated Every Day by the Strange Bureaucrats of the Intelligence Community

(By Tad Szulc)

Americans have always believed that the right to privacy is sacred. We shudder at stories told by travelers to the Soviet Union and other dictatorships who take for granted that their hotel rooms and phones are bugged and that they are followed. But now we discover there is literally no place within the United States safe from the illegal snooping of the CIA (which is restricted by law to foreign operations) and the many other government agencies known as the "Intelligence Community."

One extraordinary example is the tiny laser-beam transmitter embedded in the wall of the Oval Office at the White House. This transmitter picked up and relayed to a remote recording center every conversation between Richard M. Nixon and his aides, friends, and visitors during at least several months in 1970, the year the former president launched his secret domestic intelligence program. Presidential telephone conversations, including those conducted over "secure" scrambler lines, were also picked up by the laser transmitter.

The existence in the presidential office of this highly sophisticated device, known by the code name "Easy Chair," remains one of the most sensitive, closely guarded, and intriguing secrets of the Nixon period. This knowledge is restricted to about a dozen key past and present officials of the Intelligence Community. But the precise purpose of the operation, the exact identity of those who ordered the installation of the laser device under a coat of fresh paint on the Oval Office wall, and the ultimate disposition of the instrument remain unclear. Nor do we know if tapes were made of these transmissions—which is perhaps, the most crucial question.

It is also not known if Nixon himself was aware of and consented to the installation. If he did, the laser system complemented his hidden recording devices that produced the famous White House tapes. (In any event, the laser device picked up with infinitely more clarity every word uttered in the Oval Office, eliminating the "unintelligible" gaps that affected the tapes. In addition, the laser system permits, unlike a tape recorder, the identification of every individual voice in a room and the separation of several simultaneous conversations.) It is not known where the laser beam signal was received, but technical experts believe that such a device has a transmission range of under a half mile along a clear line of sight. The laser beam must be aimed out a window—it would be deflected by a wall. In the case of the Oval Office it had to go through the panes of the French doors leading to the Rose Garden.

Highly reliable sources told *Penthouse* that one or more senior officials of the Secret Service and the Central Intelligence Agency are familiar with the "Easy Chair" situation in the White House, although they could not say whether they learned of it only when the laser device was discovered and removed early in August 1970, or whether they knew at some earlier date. The sources would not rule out that the late J. Edgar Hoover, then director of the Federal Bureau of Investigation, was also privy to "Easy Chair."

In any event, this super-bugging of the presidential office looms as one of the most bizarre episodes in the still unfolding story of domestic spying carried out by six successive administrations, but climaxing most spectacularly during Nixon's tenure.

Penthouse learned of this bugging of the Oval Office as a result of a lengthy investigation. According to highly authoritative sources, the person who installed the laser transmitter, possibly on a second attempt when an original device did not function properly, is a foreign-born individual employed as a painter by the government and apparently controlled by one of the intelligence agencies. His name as well as a number of other relevant details are withheld from publication to avoid causing suffering and embarrassment to persons innocently involved in this operation.

Investigations by *Penthouse* have also produced the significant fact that officials of the General Services Administration, which is responsible for the maintenance of government buildings, have been under strict orders from the Secret Service since 1970 not to discuss with outsiders anything pertaining to the painting of the interior of the White House. The Secret Service also issued orders that all inquiries on the subject be immediately reported to it. These orders apply to painting foremen and their crews as well as to other GSA employees. *Penthouse* sources were unable to say, however, whether these orders are exclusively related to the "Easy Chair" incident.

Beyond the new disclosures of White House bugging, recent investigations, including those by *Penthouse*, also strongly suggest that the cover-up of secret domestic spying activities by U.S. intelligence agencies has continued in 1975, despite President Ford's instructions that all relevant information be supplied to the investigating panels: the Rockefeller Commission and two special congressional committees. But the White House has excluded certain top-secret material from information given to the Senate and House panels. These are the facts:

Civilian and military intelligence agencies maintain political files on tens of thousands of American citizens, ostensibly for reasons of "national security" and criminal investigations, but just as often to satisfy the political curiosity of overzealous government sleuths. There are files on sexual, drinking, and other personal habits and problems of politicians, government officials, artists and writers, civil rights militants, dissidents in general, and real or suspected radicals.

Court records, disclosed in April of this year (months after Ford ordered the investigation of the Intelligence Community), show that at least twenty federal agencies still maintain electronic surveillance of Americans at home and abroad. Overseas, particularly in Germany, the targets are U.S. military personnel. This surveillance includes telephone tapping and the secret recording of face-to-face conversations either through hidden devices or informers secretly wired for sound. (It is unclear, however, whether all this surveillance is based on court orders or is conducted illegally.)

The immense scope of this activity can be appreciated from this list of agencies engaging in domestic and foreign electronic surveillance of Americans: the FBI; the CIA; the National Security Agency; the Defense Intelligence Agency; the Department of the Air Force; the Postal Inspection Service; the IRS Intelligence Division; the IRS Inspection Service's Internal Security Division; the Drug Enforcement Administration; the Treasury's Bureau of Alcohol, Tobacco, and Firearms; the Naval Investigative Service; the Administrative Services Section of the Joint Chiefs of Staff; the Defense Mapping Agency; the Defense Nuclear Agency; the Defense Security Assistance Agency; the Defense Supply Agency; the Defense Civil Preparedness Agency; the Defense Advanced Projects Agency; the Defense Communications Agency; the Defense Contracting Audit Agency; the 502nd Army Security Agency Group; the Office of the Deputy Chief of Staff for Intelligence of the U.S. Army in Europe; the Investigation and Police Information Division of the U.S. Army in Europe; the Army Criminal Investigation Command; and the Defense Investigative Service. *It must be kept in mind that all this*

spying is outside normal criminal surveillance by law enforcement agencies. In addition, acting on requests from nineteen federal agencies and scores of local law enforcement units, the U.S. Postal Service (which has an intelligence unit) is currently tracing and recording the origins of mail delivered to thousands of American citizens. Our government, from the federal down to the state and municipal levels, appears to have embarked on a veritable snooping binge. (It should be recorded, however, that the Pentagon makes a point that *only* five of its agencies are authorized to conduct electronic surveillance.)

CIA director William E. Colby informed President Ford of possible illegal activities by his agency, including domestic spying and conspiracies to carry out assassinations of foreign leaders, only after a part of the veil of secrecy was lifted in press reports last December. This information had been withheld for nearly two years even though former CIA director James R. Schlesinger, now secretary of defense, ordered CIA employees as far back as 1973 to report to him activities exceeding or violating the CIA charter. He received a number of such reports. Colby inherited this material in 1973 and secretly requested the Justice Department to investigate illegal CIA actions—raising the possibility of criminal prosecutions against certain CIA officials—but he reportedly failed to inform Ford of it until the presentation of his fifty-page written report last December and his supplemental "oral" report on assassinations.

The CIA maintains its own secret list of enemies, known as the BIGOT file, in addition to 10,000 name files of Americans suspected in some manner of foreign intelligence connections or some vague form of subversion. The latter list includes antiwar and civil rights activists. *Penthouse* reported in its June issue that the CIA maintained since the 1950s separate dossiers on the late senators Joseph McCarthy and Robert Kerr, as well as on Senator Hubert H. Humphrey—in addition to New York congresswoman Bella Abzug, the only member of Congress that the CIA has publicly admitted keeping a file on. The BIGOT file is made up of persons who are regarded as "bigoted" against the agency.

Besides keeping dossiers on thousands of Americans, the CIA is also known to have maintained surveillance on Supreme Court Justice William O. Douglas; Representative Claude Pepper, Florida Democrat; former representative Cornelius Gallagher, New Jersey Republican; and the late senator Edward Long, a Missouri Democrat. The CIA's interest in Douglas and Gallagher was apparently based on their contacts in the Dominican Republic. Douglas visited there in 1962 and had close ties to former president Juan Bosch, one of whose advisers had CIA links of his own. (And allegations have been made that the CIA played a role in the 1961 assassination of the Dominican dictator, Rafael L. Trujillo.) Pepper was reportedly a target because of his ties to Cuban refugees in Florida, a major area of CIA operations. Long, according to sources, aroused the agency's interest because of links to foreign corporations operating in the United States.

CIA sources say that many "enemies" on the BIGOT list have been targets of agency bugging by "Easy Chair" laser devices. The advantage of such devices is that they are usually untraceable and do not constitute actual wiretapping for which, at least in theory, either a

court order or a "national security" clearance by the attorney general is required.

The government secretly condoned the production of awesome anti-personnel explosive devices, such as flashlights and telephone receivers loaded with explosives, by the B. R. Fox Company, a private company in Alexandria, Virginia. Some of the officials of this company are believed to have had past ties with the CIA's paramilitary operations branch. There is no evidence that B. R. Fox, which mysteriously went out of business last November, was actually owned by the CIA. But Fairfax County authorities reported upon inquiry that the company never requested nor received the necessary permit for the manufacture of explosive devices in the Fairfax jurisdiction. Intelligence sources indicate that other such companies are presently operating elsewhere in the United States.

The CIA obtained from the Civil Aeronautics Board and the Federal Aviation Administration a special certification for one of its "proprietary" airlines, Southern Air Transport Inc., exempting it from the requirement of flying approved charter routes. Southern's aircraft are thus able to be used anywhere in the world without filing route reports with the CAB.

To deal with pressures from current investigations, the CIA established at its headquarters last February a secret "CONFOUND Task Force," designed to counter charges against the agency. CONFOUND is supported by CIRA, the Central Intelligence Retired Association, formed last March 20. CIRA's board of governors includes some of the best-known former senior agency officials. The CIA, according to informants, also sought to plant at least two of its former officials on the staff of the Senate committee investigating the Intelligence Community.

Its naval operations ranging from the sublime to the rediculous, the CIA has been involved with billionaire Howard Hughes in various ventures, including the ship designed to retrieve a sunken Soviet submarine, and it continues to operate—from a room in a small New York hotel and from a postal box in Panama—the *Apollo*, a mysterious motor yacht loaded with electronic and communications equipment. The 3000-ton *Apollo*, which is almost 500 feet long, usually operates in southern European waters.

This article will examine in some detail the domestic activities of the U.S. Intelligence Community—many of them clearly illegal and a clear and present danger to the democratic process.

For over twenty-five years these activities have often been in direct violation of U.S. laws. (The CIA, for example, is barred by federal law from domestic intelligence operations and from domestic police functions.) In addition, this domestic espionage has violated the civil rights of Americans on whom secret political files have been kept, whose phones have been tapped with or without court orders, and whose mail has been opened or, at least, monitored through Postal Service "mail covers" on behalf of various intelligence agencies. And there have been many unexplained accidents, deaths, and "suicides" in the U.S. involving persons who had connections with intelligence work.

Moreover, the intelligence agencies, using their immense manpower and financial and technological resources, have been part of great

political power struggles in this country going back at least ten years. "Keeping files on citizens may be the least some of these agencies have been doing," an intelligence expert with long experience in Washington remarked recently.

Some major American political assassinations, on which official files have been closed, may become the subject of new scrutiny by Rockefeller and the special congressional committees. If nothing else, a psychological climate has developed favoring the reopening of investigations of the murders of the Kennedy brothers and the Rev. Martin Luther King.

This climate, in which the CIA and the FBI are being publicly linked to these and other political assassinations, evidently led President Ford to remark at his news conference on April 3 that "it is my understanding that the Rockefeller Commission may, if the facts seem to justify, take a look" at the charges that the CIA was involved in the 1963 murder of President Kennedy and that it was a conspiracy involving more than one gunman. This would be the first fresh official look at the Dallas assassination since the Warren Commission issued its report more than eleven years ago declaring that Lee Harvey Oswald was the lone assassin.

Ford, who was a member of the Warren Commission, said that "so far" he has seen no evidence to dispute the original conclusions. David W. Belin, executive director of the Rockefeller Commission and formerly counsel to the Warren Commission, took the same view. (But George O'Toole's recently published book *The Assassination Tapes*, which was excerpted in the April *Penthouse*, presents what may be called the first scientific evidence that Oswald was innocent.) Meanwhile, the Rockefeller Commission has received allegations in form of testimony from private groups that E. Howard Hunt, the ex-CIA official and convicted Watergate burglar, had been arrested in Dallas minutes after Kennedy's shooting. Hunt has denied this charge as well as published reports that he was in Mexico City in August 1963, at the same time as Oswald (see Hunt Interview, *Penthouse* May 1975).

There are also new doubts surrounding the murder of Robert F. Kennedy in Los Angeles in June 1968, and the special investigating bodies may look into it, too. Charges of CIA and FBI involvement in the 1968 assassination of King in Memphis were made early in April by the Rev. Jesse Jackson, who succeeded King in the leadership of the civil rights movement. This accusation coincided with recent assertions by James Earl Ray, the convicted assassin, that he did not act alone and with his request for a new trial. Acting on Hoover's orders, the FBI had been wiretapping King during the years preceding his death. A Hoover memorandum, disclosed several years ago, said the FBI's mission was "to disrupt, discredit, or otherwise neutralize the civil rights movement."

Political power struggles may have also been behind the installation of the "Easy Chair" laser device in Nixon's office in 1970. This secret transmitter is similar to the one accidentally discovered many years ago inside the Great Seal of the United States in the office of the American ambassador in Moscow. Such devices, unlike standard hidden microphones and transmitters, cannot be located by electronic

sweeps. The instrument in the Oval Office was apparently discovered by a Secret Service agent who noticed an extra dab of paint covering the spot on the wall where the device was implanted. The paint caught his eye because of the way in which the light was being reflected by it at that particular moment.

It is possible that Nixon had personally ordered the implanting of the laser device to obtain a more accurate secret record of all conversations in the Oval Office and chose to keep the Secret Service in the dark about it. But it is also possible that, because of the extraordinary importance of policy decisions made in the Oval Office, one of the intelligence services may have installed the device. (There is at least one other case of such spying in the White House: during 1971, a navy yeoman attached to a Pentagon liaison office in the National Security Council regularly supplied the Joint Chiefs of Staff with the most top-secret materials from NSC meetings as well as the most sensitive foreign policy documents handled by Henry A. Kissinger, who then served as special assistant to the president for national security affairs.)

The Oval Office transmissions could be monitored anywhere in the White House or the adjoining Executive Office Building. They could also be picked up, technicians say, in the Treasury Building a block away (the Secret Service is part of the Treasury Department) or in the Commerce Department building three blocks away. But, because laser beams can travel only along a line of sight free of any obstructions, it would be necessary to have "repeaters" located somewhere on the White House grounds to redirect the beam emanating from the Oval Office windows to reception points. If, indeed, the president was spied on by one of his intelligence agencies, the American government was in a greater state of disintegration than we ever realized.

Policy power struggles likewise seemed to loom behind the CIA's own violent reorganization in the wake of the disclosures last December that the agency had engaged in "massive" spying on Americans. CIA director Colby, anxious for a scapegoat, apparently chose the chief of the Counterintelligence Staff, James Angleton, as the public culprit, although knowledgeable agency officials believe that Angleton had relatively little to do with it. The belief in the Intelligence Community is that the spying scandal gave Colby the long-awaited opportunity to dismiss Angleton, a powerful operator who had carved out his private empire in the CIA. Angleton had become a thorn in the side of Secretary of State Kissinger because of his control over the flow of secret intelligence between the U.S. and Israel. Kissinger, it is said, felt that Angleton was interfering with his intricate Middle Eastern policies and persuaded Colby to remove him as soon as possible.

Angleton was quietly replaced by George Constantinides, a fifty-three-year-old Middle East specialist who has directed the CIA's Near Eastern Affairs Office since 1972, and is unlikely to create problems for Kissinger. But nothing was said about Richard Ober, the official who ran the CIA's Domestic Operations Division (renamed the Foreign Resources Division in 1972) during the period when the agency was engaged in spying on antiwar militants. Ober currently is assigned to the National Security Council staff where, presumably,

he enjoys Kissinger's protection. Angleton, who stayed on for three months to assist Constantinides during the transition, was awarded on April 7, 1975, the CIA's Distinguished Intelligence Medal in a surge of bureaucratic irony. Colby managed to be in New Orleans on the day of the award and Angleton received it from Colby's deputy, Lieutenant General Vernon A. Walters. Another power struggle had run its course.

As we've noted, the CIA is forbidden by federal law to operate in the United States except for managerial, policy, training, and support functions related to its foreign operations. But this prohibition has been violated to a steadily increasing degree since the CIA was founded twenty-eight years ago. The violations range from supporting local police departments and spying on American citizens to managing a huge corporate empire, shielding mysterious private companies producing lethal devices for use at home and abroad, supplying tax covers for such companies as Howard Hughes' Summa Corporation, which built the submarine-recovery ship *Glomar Explorer* (it saved Hughes over $9 million), and conspiring on United States soil to commit foreign assassinations. Conspiracy to commit murder is a major criminal offense under the United States Penal Code (it probably would be considered a federal rather than a state offense because such murders would most likely be planned in a federal office) and current investigations by the Justice Department could lead to indictments of CIA personnel.

If this happens, one may well ask why "higher-ups" in the government, including members of the White House "Forty Committee," which must authorize foreign assassinations by American agents, would not be liable to prosecution. The Forty Committee is presently headed by Henry Kissinger and a case of legal accountability may develop against him and his predecessors. It may even be argued that presidents of the United States can be named as co-conspirators in foreign assassinations, inasmuch as they supposedly must clear such acts when Americans are used. But traditionally presidents have been protected by the so-called doctrine of "plausible denial," under which they are able to officially ignore this type of activity. Moreover, the Forty Committee keeps virtually no records, thus depriving courts of needed evidence. And no official is likely to incriminate himself in court—should it ever come to that.

It is obviously impossible to separate completely the CIA's domestic and foreign activities. The agency, after all, has its headquarters in the United States and all its operations are planned and coordinated at its sprawling building at Langley, Va., just outside Washington. Because of all the support requirements at home, the CIA's operations inevitably spill over to American cities. It is this spill-over factor that has often led to the abuses and violations.

The CIA claims that it acts legally on American territory when it engages in training and recruitment, the contacting of Americans and foreigners who may possess useful intelligence information, and the investigation of potential agents or informers it may wish to hire (as distinct from campus recruitment for CIA careers). Few CIA critics would dispute this claim. Likewise, there appears to be nothing wrong with the work here of the agency's Technical Services Division, which

concentrates on intelligence technology and the equipping of agents for foreign missions, or the Office of Security, which supposedly does what its name suggests. In fact, "overt" CIA offices in dozens of American cities are listed in local phone directories.

The trouble, however, is that the CIA also runs "covert" offices and operations throughout the United States—the ones Colby does not mention in his increasingly frequent public appearances in defense of the agency. Here are five examples:

1. The Miami area is the center of major covert CIA operations. The principal operation is Support Station East, headed by a senior CIA official named Paul Holliwell, in charge of all the activities in Florida. A special section deals with anti-Castro Cuban refugees, many of them veterans of the Bay of Pigs invasion and other CIA adventures in Cuba. The Cubans are used as intelligence sources and as infiltrators into Cuba (although this activity has been considerably curtailed over the years). Eugenio Martinez, one of the Watergate burglars, was still on a $100-a-month CIA retainer when he joined E. Howard Hunt's Cuban-American team for Beverly Hills and Washington break-ins. All the other Hunt accomplices were ex-CIA personnel. Miami law-enforcement authorities remain highly concerned about the activities of CIA-connected Cubans, many of them armed, in local crime. There is talk of a "Cuban Mafia" using CIA Cubans, and there have been numerous instances of terror bombings and assassinations. But the local police and even the FBI often find that some Cubans with criminal records are "untouchable" because of CIA protection and invocation of "national security."

"Support East" uses the facilities of Miami International University for operations in Latin America and provides technical and financial support for far-flung CIA missions. But, most important of all, it controls a worldwide network of double agents under Operation SEEBOLT, one of the most sensitive CIA missions. A special staff known as the "Green Light Group" runs SEEBOLT on behalf of the agency's Clandestine Services chiefs in Washington. It is in close touch with the Inter-Agency Defectors' Committee (IDA), a major source of double agents. Despite many valid objections to turning an American city into a major espionage center, CIA officials insist privately that this activity is all really part of foreign operations.

The Miami group has its counterpart, Support Station West, in Burlingame, California. This station, near San Francisco, concentrates on Asian operations in roughly the same manner in which the Miami station works on Latin America and Europe. There is also a large covert CIA station in Denver, and there is one in Las Vegas, where the Mafia provides a fertile field for foreign and domestic intelligence.

2. In the overlapping of the CIA's foreign and domestic functions, the agency's representatives in Los Angeles first persuaded Howard Hughes' Summa Corporation to build the $350 million (in taxpayers' money) deep-sea mining ship, the *Glomar Explorer*, and then went to the Los Angeles County tax assessor to inform him in secrecy that the vessel belonged to the United States government. The Summa Corporation thus was not subject to local taxes in excess of $9 million. But this is where the CIA got caught in its own game of secrecy: the ship's license, filed under oath with the Coast Guard, states that the

Glomar Explorer belongs to the Hughes interests. Los Angeles County was thus cheated out of taxes. Inasmuch as the CIA did the lying, it may well become the target of tax fraud prosecution. The same may happen with federal taxes, although the IRS has not yet been heard from, and we may face the extraordinary situation of a federal agency (IRS) suing another federal agency (CIA) for tax fraud. And there is the additional fact that the CIA representatives were introduced to the tax assessor by an FBI agent, suggesting further intra-governmental collusion. The CIA's request that the tax assessor cooperate in the secret cover is another example of the agency's domestic activities that often verge on the illegal.

This story is further complicated by Global Marine Inc., a publicly held company (unlike the Summa Corporation) which designed and operated the *Glomar Explorer* for Summa and the CIA. Under Securities and Exchange Commission rules, public companies must provide "full disclosure" of their activities. Global Marine chalked up profits from the *Glomar Explorer* operations, but, according to an SEC staff study, its public reports were "inaccurate and incomplete due to the classified aspects." Thus far the SEC has avoided making a broad ruling on Global Marine's public reporting. If one is made, however, it would affect other public companies with secret CIA contracts, possibly blowing their covers.

3. In the CIA's operation of its vast corporate activities—the so-called "proprietary" companies—the agency has always badly needed the secretive cooperation of federal and state authorities. It is, of course, a matter of subsequent legal determination whether the incorporation of the proprietaries and their operations have been in violation of laws. The existence of the CIA corporate empire, estimated at some $200 million annually in sales and services, has long been a secret and there have been no court tests of the legality of these proprietary companies. Since none of these companies has publicly owned stock, problems with the SEC are unlikely to arise.

The CIA began putting together its proprietary corporate network in the early 1950s in order to acquire domestic and foreign covers for secret operations and to channel funds discreetly to its overseas operatives. Only top CIA officials know how many of these companies are or have been in existence—what is known of the operation suggests that the agency has been closing down some of them and creating others, according to need—but the system is being used to this day. Colby, in fact, confirmed it earlier this year when he denied a charge that profits generated by the proprietaries can be used for covert foreign operations, thus bypassing restrictions written into law by Congress late in 1974.

Most of the proprietaries were incorporated in Delaware, a state that does not levy local corporate taxes, and there are reasons to believe that the CIA even has its own incorporating company in Dover to handle the business away from prying eyes. CIA officials say, however, that in some instances officials in the office of the Delaware secretary of state had to be informed of the true nature of the proprietaries to avoid blowing the CIA covers.

Probably the oldest major proprietary is the Pacific Corporation, with headquarters in a third-floor suite in an office building at 1725

K Street in Washington. Incorporated in 1950, Pacific is one of the principal CIA holding companies because it provides financial and management controls for other important proprietaries. Pacific's president is Hugh L. Grundy, believed to be a longtime CIA official, who actually lives just a few blocks away from the agency's Langley headquarters.

Operating directly under Pacific are Air America, Inc., the "private" CIA airline that has operated planes and helicopters for years throughout Indochina in support of the agency's "clandestine army" in Laos and other paramilitary activities. Air America is funded by the Agency for International Development (AID), which has often served as a cover for the CIA's operations in Asia and elsewhere. The CIA refunds AID through a complex bookkeeping system involving the concealment of CIA appropriations throughout the federal budget.

Pacific also owns Civil Air Transport Co. Ltd., a Taiwan-based scheduled airline known as CAT. CAT, in turn, owns major aircraft repair and overhaul facilities on Taiwan. The third known CIA airline is Southern Air Transport Inc., which is also the most mysterious. Southern (not to be confused with Southern Airways), located at 1625 K Street in Washington (in a building with a number of unusually large antennas on the roof), has interlocking directorships with Air America. Between 1966 and 1972 it leased aircraft from Air America as well as from Air Asia Co. Ltd., another proprietary controlled by Pacific. According to Federal Aviation Administration records, the present ownership of at least four jet transports leased from Air America and subsequently returned to it is "unknown." These planes, in fact, are not even registered anymore with the FAA. At present, Southern owns three transport planes, one of them a DC–6 (bought from Air Asia). A DC–6B was sold to Ethiopian Airlines in 1972.

(Southern's attorney is James H. Bastian, who is vice-president and secretary of the Pacific Corporation. Bastian, incidentally, is the registered owner of several apparently uninhabited townhouses in Washington.)

Most of Southern's operations have been in Latin America, including eight flights to Chile in 1971 (on earthquake relief missions for LAN, the Chilean national airline, according to a CAB certification) when the late president Salvador Allende was still in power, but very little is known of the current use of its planes. Its operational headquarters are in Miami, but at one point Southern was leasing one of its aircraft to a U.S. oil company working in the Niger in Africa and another to a company in Alaska.

Late in 1973, Southern was officially for sale and it filed a petition with the CAB for "cancellation of certificates" for charter routes. But the airline then changed its mind, and on December 31, 1973, became a "commercial operator" under FAA Regulation 121. No longer under the CAB's operating authority, Southern has greatly increased its anonymity—it no longer has to file documents showing aircraft purchased or sold, detailed financial statements, and a log of all civil operations listing the number of hours flown by aircraft types, tonnage carried on each route, intermediate stops, and the number of trips made over each route. As a "121" contract operator, Southern has no restrictions on where it may fly—except those by foreign governments. Under

the new status, Southern cannot advertise for commercial work, but this seems to be the least of its worries.

Other Pacific subsidiaries include the Pacific Engineering Co. and the Thai Pacific Services Co. Ltd. The nature of their activities is unknown. Foreign Air Transport Development Inc., another proprietary, has gone out of business. And over the years the CIA and its subsidiaries have dealt with such companies as Lao Air Development Inc., operating in Laos under Air America, and Birdair, the company that flew the Cambodian airlift for the U.S. air force in 1974 and 1975.

Acting through other channels, the CIA had been funding since 1965 a Washington firm named Psychological Assessments Associates, Inc., whose function was to conduct psychological assessments of American citizens hired for foreign employment and to study brainwashing techniques of foreign intelligence agencies. PAA was organized by two former CIA officials, Samuel B. Lyerly and Robert E. Goodnow. (Goodnow has since gone to live in Australia for unexplained reasons.) PAA operates in complete secrecy. Admission to the office, in a residential uptown section of Washington, is obtained by pushing a buzzer so that the door may be opened. But PAA's present directors are not available for interviews and the CIA has refused comments on its links with the company.

As a rule, CIA proprietaries pay taxes and meet other official requirements, but CIA director Colby had to arrange for a special dispensation from the now defunct Price Commission so that Pacific Corporation's books would not have to be opened for the commission's inspection.

In addition to proprietaries, the CIA runs "fronts" and "conduits" through companies it does not run outright but supports financially. The fronts and the conduits provide covers for CIA operations at home and abroad. The best known of the fronts was the now disbanded Robert R. Mullen public relations company that employed E. Howard Hunt after his resignation from the CIA in 1971 until his involvement in the Watergate break-in. Interestingly the Mullen company also handled a public relations account for the Howard Hughes interests. The company, as it developed in 1974, was controlled by a full-time CIA case officer. There are many other such fronts.

Some of the most interesting CIA conduits—channels for transmission of funds and other materials—were the German companies broken up after the war by the Allied military authorities. These companies included such giants as the Farbenindustrie A.G., the huge Nazi conglomerate, and there are indications that the CIA planted its agents in new firms resulting from postwar decentralization, including their United States subsidiaries. These and other companies—some of them famous American business institutions—serve the CIA through the supply of invoices for materials and services that were never rendered so that money can be easily shifted abroad for the agency's operations. It was through the branch offices of a large New York-based banking and currency firm that the CIA sold dollars for piastres in the black market in Vietnam.

4. The case of the B.R. Fox Company. According to its letterhead this company specialized in "custom designed electronic specialties," but in reality it manufactured lethal explosive devices. As noted

earlier, there is no direct evidence to connect Fox to the CIA. However, one of its directors, Michael Morrissey, had past links with the CIA's Paramilitary Operations Branch, according to agency officials. It is also known that Morrissey, according to memoranda written by him, had been in contact with Lieutenant Colonel Lucien Conein, a former senior CIA official currently serving with the Drug Enforcement Administration (DEA). Conein admitted to newsmen that he had been approached by Morrissey, but insisted he never became involved in any dealings with him.

Fox, which operated from a warehouse at 2701 Fairview Drive in Alexandria, Virginia (it also had an office at 15 Abingdon Square in New York City), produced a line of "Astro" horror items. These lethal devices included explosive-filled telephone handsets, booby-trapped magazine clips for the M–16 rifle, flashlights and cigarette packs full of explosives, a "fragmentation ball," and an exploding camera.

Fox's catalogue notes that "the information contained herein is CLASSIFIED by the manufacturer for U.S. Government use only. The handling and storage of this material should be done so mindful of its sensitive nature." This is how the explosive phone handset device is described: "Size 1.25″ x 0.75″ x 0.5″. Use of the inside telephone handset. Automatic charge fired at (blank) seconds following lifting of instrument handpiece. Easy and quick installation to underside of mouthpiece. Any desired time delay can be preset. No switches, presetting, or batteries. Simply install 4-wire module. . . . Miniature unit . . . rugged and durable. All hand wired. Unlimited lifetime with proper handling."

The exploding cigarette pack, described as an "anti-disturbance explosive," functions as follows: "Electronics and explosive module packed inside cigarette pack. When the pack is lifted or moved in any manner, the explosive is set off. Simple operation. Only one switch. . . . A built-in electronic counter is factory set for 90 seconds to allow time for evacuation of the area. . . . The circuit will stay armed for a period of 2½ to 3 years. . . . Explosives are not included and is the only thing to be added." In the flashlight, the catalogue explains, the "normal On/Off switch on the side activates the operation." Then the catalogue adds: "This is an example of an explosive anti-disturbance dummy unit. Any other items desired to be so modified may be submitted for such evaluation."

That the CIA may have been the intended, if not actual, client for the Astro line is suggested in Fox's classified catalogue, which says that the explosive devices "have been designed and manufactured for sale to authorized agencies of the United States government specifically intended for application outside of this country." A well-informed government official remarked in an interview that "I can't think of anybody outside the CIA who would want to buy this kind of stuff—and I'm not even sure the CIA would." But the mystery remains: if the CIA was not the client, for whom was Fox working? Moreover, as we've said earlier, Fox never requested or obtained the required license for manufacturing explosives in Fairfax County. How did Fox get around it?

Nobody seems to know what has happened with these assassination devices after Fox Company suddenly went out of business. It may

be something the Rockefeller Commission and the congressional committees will wish to explore as they look into charges that the CIA has been involved in foreign assassination plots.

5. The CIA is explicitly forbidden by law to exercise domestic police functions. But it has secretly collaborated with numerous police departments throughout the U.S. in support of their political intelligence functions. One of the most notable examples was the agency's "formal liaison" with the Metropolitan Police Department in Washington, D.C., going back to the late 1940s. Maurice J. Cullinane, the new MPD chief, acknowledged in a report last March that the Washington police borrowed agents, automobiles, and electronic surveillance equipment from the CIA to help them spy on political activists in the capital. This "Cullinane Report" was one of the most detailed admissions by any U.S. police department on its political intelligence work. The department's intelligence division spent $1.7 million since 1968 on political surveillance. The relationship between the CIA and the Washington police became particularly active in 1969, when the agency trained at least seventeen MPD officers, twelve of them in "intelligence activity." The CIA gave the department what was described as "two lamps capable of intercepting oral communications." Even the department's morals squad received wiretap devices from the CIA. Between 1968 and December 1974, the Washington police had also been training "selected CIA employees" in interrogation techniques. Police departments in the Washington area have also provided CIA officials with local police credentials to facilitate domestic undercover work.

Former CIA director James Schlesinger suspected the CIA may have been engaging in illegal activities shortly after he replaced Richard M. Helms, now U.S. ambassador to Iran. In an internal memorandum to "all CIA employees" sent out on May 9, 1973, Schlesinger said:

"I shall do everything in my power to confine CIA activities to those which fall within a strict interpretation of its legislative charter. I take this position because I am determined that the law shall be respected and because this is the best way to foster the legitimate and necessary contributions we in the CIA can make to the national security of the United States. I am taking several actions to implement this objective: I have ordered all the senior operating officials of this Agency to report to me immediately on any activities now going on, or that have gone on in the past, which might be construed to be outside the legislative charter of this Agency. I hereby direct every person presently employed by CIA to report to me on any such activities of which he has knowledge. I invite all ex-employees to do the same. Anyone who has such information should call my secretary (extension 6363) and say that he wishes to talk to me about 'activities outside CIA's charter.' . . . Any CIA employee who believes that he has received instructions which in any way appear inconsistent with the CIA legislative charter shall inform the Director . . . immediately."

Schlesinger evidently received substantial response to his request because Colby, when he succeeded him later in 1973, began turning evidence over to the Justice Department for investigation and possible prosecution. However, for reasons that remain unclear, Colby appar-

ently failed to notify the President of his move. Ford became aware of it only after the domestic spying scandal broke out late in 1974.

Subsequently, David Blee, deputy director of the CIA's Directorate of Operations (Clandestine Services), advised CIA employees by memorandum that they should retain private counsel in the event of legal proceedings against them in connection with the Justice Department's investigation.

But the CIA is not alone when it comes to illegal domestic political operations aimed at American citizens. The FBI, as we now are beginning to discover, was among the culprits. The new attorney general, Edward H. Levi, told a congressional subcommittee earlier this year that J. Edgar Hoover had amassed at least 164 files containing folders with information, some of it derogatory, on "presidents, executive branch employees, and seventeen individuals who were members of Congress." The files were marked "OC," meaning "Official and Confidential." Levi added that the existence of these files was not made known by the FBI to the Justice Department, of which the FBI is a part, until early 1975. In other words, the Hoover files were a secret from dozens of attorneys general over the years. (The present FBI director, Clarence M. Kelley, never told Levi's predecessor, former attorney general William B. Saxbe, about them.)

Under a secret program known as COINTELPRO, initiated by Hoover in 1956, the FBI ran for years a counterintelligence operation aimed at domestic dissenters. Although the program was formally terminated in April 1971, these activities, including the harassment of radicals, went on at least until 1973. Among COINTELPRO's targets were the Socialist Workers' Party, the Young Socialist Alliance, the "New Left," American Communists, "black extremists," and "white hate groups." COINTELPRO was originally aimed at foreign intelligence agents in the United States, a proper FBI function, but Hoover, without clearance from successive attorneys general, applied it to domestic groups as well.

In 1969, for example, the FBI sent a fake threatening letter to a black Baptist minister, Donald W. Jackson, to force him to abandon his civil rights work at Tougaloo College in Mississippi. The letter was sent in the name of a nonexistent "Tougaloo College Defense Committee," whose members were said to be armed. And in 1972, a Florida resident was recruited by the FBI to infiltrate and disrupt radical groups in the United States and Canada. The informant, Joseph A. Burton, told newspaper interviewers that as late as 1974 he was told by the FBI of its efforts to put the Vietnam Veterans Against the War out of business in Florida.

One of the FBI's most astonishing unauthorized efforts was against the small Socialist Workers' Party and its affiliate, the Young Socialist Alliance. The party had not been prosecuted since 1945, but the FBI files on the disruption program runs to an amazing 573 pages. The bureau's harassment of the party reached the point where, last December, a federal judge in New York ordered the FBI to desist from conducting surveillance on a national convention of the Young Socialist Alliance. Another instance of unauthorized FBI activity came to light when it was learned that the security chief of the American Indian Movement during the Wounded Knee takeover in 1973

had been a paid FBI informer. Evidently, neither Hoover's death nor Watergate has taught the FBI anything about the need to observe the constitutional rights of Americans.

It seems as if every government agency has been involved in some form of spying on Americans. Thus the CIA, with the cooperation of postal officials, has been intercepting, reading, and copying since 1953 uncounted thousands of first-class letters written by Americans to addresses in the Soviet Union. Former CIA director Richard Helms refused to stop the interception in 1969, but Colby testified that the agency suspended the operation in February 1973. He admitted the program was "illegal." So frantic was this mail reading by the government that the CIA developed, at great cost, a special machine to unseal and reseal envelopes of every conceivable size in a matter of seconds.

During 1974 the U.S. Postal Service surveilled and recorded the origins of all mail received by nearly 4,500 Americans. The CIA was no longer requesting such mail covers last year, but the Postal Service was acting on the behalf of the Naval Intelligence Service; the Army Intelligence Command; the Air Force Special Command; the Air Force Special Investigations Office; the Interstate Commerce Commission; the Commerce Department; the Health, Education, and Welfare Department; the Agriculture Department; the IRS; the FBI; the Postal Inspection Service; the Drug Enforcement Administration; the Secret Service; the Coast Guard; the Interior Department; the Labor Department; the Justice Department; the Immigration and Naturalization Service: Customs; the Royal Canadian Mounted Police; and a vast number of local police departments and tax offices.

The Internal Revenue Service, through its special service staff, was also involved in domestic espionage. A congressional investigation established that the IRS had 11,458 files on individuals and organizations (including 706 persons from Nixon's "enemies list") for reasons that clearly had nothing to do with tax collection. In Miami, the IRS cranked up its "Operation Leprechaun" designed to assemble data on the sex and drinking habits of prominent residents, including the state's attorney.

The National Security Agency, a supersecret outfit dealing with code breaking and electronic intelligence, is currently continuing to monitor all overseas telephone calls and cables. During the Nixon period, the NSA was an enthusiastic supporter of Nixon's domestic intelligence program, particularly when it came to breaking into foreign embassies. Admiral Noel Gayler, then the NSA director, has been rewarded with the post of commander-in-chief of all U.S. forces in the Pacific (CINCPAC).

There could be an endless list of the intrusions of our government into our private lives. Let us conclude with three of the more striking examples: in 1969 Henry Kissinger recommended names of his closest aides and several newsmen to be bugged by the FBI for "national security" reasons; the CIA investigated the personal life of a Nixon campaign adviser in 1968; and a deputy attorney general proposed in 1975 that "internal passports" be issued to aliens in the United States, a step that could have led to a national identification system on the Soviet model. However Attorney General Levi vetoed the scheme.

Spying and covert activity is now an official government pasttime in the United States. Can the president or Congress arrest this trend toward an American police state? The answer is vital in determining the kind of society in which we will live.

[From Business Week, July 7, 1975]

The Erosion of Privacy

Anyone who claims he hasn't heard about the growing threat to privacy in the U.S. has obviously just returned from a long vacation on Mars. A steady stream of books, articles, lawsuits, Congressional investigations—and major revelations turning up almost daily in the headlines—cannot fail to have convinced even the least interested that an issue of immense importance confronts the nation. Why still another book on the subject?

The answer lies in the widely diverse events and activities that can be placed under the head "invasion of privacy." It takes no great leap of the imagination to understand that when the CIA read Representative Bella S. Abzug's mail—starting at least 20 years ago during a time when she was a practicing attorney—not only her privacy but that of her clients was invaded. This practice is illegal, and we all recognize that it ought to remain so. After all, if the CIA can read Abzug's mail, the FBI might want to claim that it should read the mail that the law firm of Cravath, Swaine & Moore gets from its current antitrust client, IBM.

But many people might not see a similar invasion of privacy in the recent call by the contentious director of the U.S. Passport Office, Frances G. Knight, for mandatory internal passports for all Americans. Knight thinks that if we all carry identity cards, the incidence of fraud and other forms of antisocial behavior may be reduced. Yet this proposal is of a kind with a host of governmental and even corporate practices that increasingly push the average citizen into the harsh glare of the public spotlight.

It is the great merit of *No Place to Hide* that all the seemingly diverse ways by which a person's privacy can be stripped from him are brought within the compass of less than 200 pages. More important even than the details, each of which is chilling enough, is the comprehensive picture that ultimately emerges of a democracy being picked apart by political institutions left to their own devices through the apathy of the citizenry.

Here is the story of the wiretap and the bug, with concise descriptions of more than two dozen interception devices available through the catalogue of the Sirchie Fingerprint Laboratories in Maryland and certain other distributors—the "Sub-miniature Surveillance Microphone," so tiny it will fit in the cavity of a tooth; the "Automatic Telephone-Line Interceptor," which even the telephone company, says its manufacturer, cannot detect; or the "Gus Model 1012 Vehicle Follower System" with quadraloop antenna. These devices are

as useful in locating married men who have affairs as they are in recording every statement of the political extremist.

Here, also, is the story of how your every step in life is preserved on paper in the files of credit agencies, insurance companies, doctors, and government agencies of every description. Perhaps everyone is familiar with tales of credit denied because of false information (supplied by overeager or vengeful informers) willingly accepted by credit bureaus that must fulfill quotas of rejects to make it seem as though their agents are thorough. But who knows or cares about the thousands of children born addicted to dope, because of the mother's habit, whose names reside now in the computers of the Bureau of Narcotics & Dangerous Drugs as "reformed narcotics users"?

Who knows that lie detectors, used to test private job applicants as well as potential defendants, can be manipulated to coerce false admissions? Who cares that there are criminal penalties for refusing to answer Census Bureau questions about home appliances and services supplied by landlords?

If none of these matters causes you concern, consider the destruction of roofing contractor John Conforti's $65,000 Massapequa (N.Y.) home by agents of the Bureau of Narcotics & Dangerous Drugs who had been tipped to the possibility that $4-million in drug profits was stashed away somewhere inside the house. Within 24 hours, "paneling was pried from the walls, furniture broken in pieces, patio tiles uprooted, aluminum siding ripped off, gaping trenches dug in the yard." Nothing was found; the informant had made a mistake. The agents had a warrant, but warrants do not grant authority to wreck. Could this happen to you? Would your government apologize and repair the damage? Probably not. The bureau's associate regional director was quoted as saying that he thought what had happened was "reasonable."

And if these and other incidents fail to shake you, the sections of the book on the IRS, the FBI, and the U.S. Army surely will—not only because of the outrages committed in the name of liberty but also because of the fiscal insanity of it all, such as the IRS seizure of a taxpayer's automobile to satisfy a $1.25 claim.

That said, it is a shame that this useful compendium is marred by a breathless and at times even whining tone. The facts are far more eloquent than the way the authors set them out. Editors should have caught a number of needless errors, such as locating our Constitutional privilege to petition the government for a redress of grievances in the Second, rather than the First, Amendment. And there are too many explicit surmises about motives and reasons, indicating that the authors were content to use scissors and paste, rather than the telephone, the mails, or the personal interview. Worst of all, the authors nowhere set out a coherent, consistent definition of the privacy to which they think each of us is entitled. This is the paramount question to which this nation of individualists had better address itself before the private sphere disappears altogether.

JETHRO K. LIEBERMAN.

Jethro Lieberman is BUSINESS WEEK's Legal Affairs editor.

[From the Washington Post, July 12, 1975]

Eavesdropping Tools Outflank Law

(By Jack Anderson and Les Whitten)

A chilling study for Congress suggests that Americans are closer to George Orwell's concept of 1984 than they may think.

Orwell described an advanced police state whose citizens couldn't make a move without the government knowing it.

With only nine years to go to 1984, the federal government may not yet be watching everyone, but it can concentrate an infinite variety of eyes and ears on anyone who arouses its suspicions.

A whole new arsenal of eavesdropping devices, according to the study, not only is available to government gumshoes but can be used with impunity.

For the 1968 law on the subject, thanks to the loose language drafted by law-and-order Sen. John L. McClellan (D-Ark.), places only the mildest restraints on the federal snoops.

The study was conducted by electronics consultant David Watters for Rep. Charles A. Mosher (R-Ohio). Watters' unpublished, 140-page report describes a number of devices that have turned snooping into a sinister science.

Here are just a few ways, under the 1968 statute, that the government can intrude upon individual privacy:

Electronic "scanners" can sort through telegraph, Telex and other written transmissions, pick out key words and then automatically reproduce the whole message, Watters reports.

Similar scanners can be used, according to the study, to intercept data, facsimile and video transmissions.

Devices known as "pen registers" can record the numbers dialed from a telephone, plus the date, time and length of the call.

"Certain exotic categories of switch and signal wiretapping equipment," states the Watters study, "(can) automatically sweep at high speed through thousands of communications circuits per hour searching for special signal address patterns." In other words, intricate equipment, now available, can scan whole communities, select out the call of a person under surveillance and automatically record the telephone data. Or, if the government wishes, the conversations can be recorded.

Unknown to the customers, many telephone calls are transmitted by microwaves which can be intercepted without even the telephone company knowing it.

Under the 1968 act, oral interceptions are supposed to be forbidden. But the language refers only to the actual voices, not to the telephone data that can be intercepted without qualms.

As Watters puts it: "The citizen has no defense against the invasion of his privacy by switch and signal type telephone tapping."

With court permission (often no more than an okay from a go-along county magistrate), law agencies can engage in even more spectacular eavesdropping.

In the future, police in hideaways will be able to intercept laser beam transmissions and even pick up the minute impulses of computers and electric typewriters.

To protect privacy, the Watters report recommends that "all wiretapping in the United States should be limited to . . . the Federal Bureau of Investigation."

Even though the FBI has abused the law, it is still, in Watters' opinion, "the only agency in our country to whom we can safely entrust the privilege of intercepting wire and oral communications."

As a guard against FBI abuses, Watters would require the FBI to obtain a court warrant not only for routine wiretapping but for all other forms of electronic interceptions. Then after the eavesdropping had ended, the subjects would have to be notified and the eavesdroppers would have to be identified.

Congress is unlikely to go as far as Watters wishes. But Sen. Charles McC. Mathias (R-Md.) and Rep. Mosher have introduced legislation to close the most gaping loopholes in the 1968 law.

[From the Washington Post, June 18, 1975]

The Loss of Privacy

(By William Raspberry)

The technicians have it in their power to learn everything that anybody, anywhere knows about us—which is to say, virtually anything worth knowing.

And if it's true that anything that *can* be done sooner or later *will* be done, individual privacy will shortly be dead as a dodo.

For a good many of us, it may be dead already. NBC's Ford Rowan, in a recent series of television reports, told us that the files the military collected on demonstrators and dissenters, supposedly destroyed after their existence became known, in the late 60's were in fact copied and have been distributed to who-knows-how-many agencies.

And while what was copied and distributed may have been isolated bits of seemingly irrelevant data, government technicians also have it in their power to put it all together—to construct instant dossiers on, as Rowan put it, anyone who has ever paid taxes, used a credit card, driven a car, served in the military or been arrested.

What makes 1975 different from 1968, when the Congress was rejecting a proposal for a national data bank, or even last year, when Fednet—a plan to link up the computers of various federal agencies—was killed, is: Now it can be done. Quickly and easily.

The key breakthrough is something called the interface message processor, or IMP. According to newsman Rowan:

"Different computers communicate in different computer languages. Before the IMP, it was enormously difficult, in many cases impossible, to link the various computers. The IMP, in effect, translates all computer messages into a common language; that makes it very, very easy to tie them into a network."

Rowan says such a network is in fact in operation, providing "the White House, the CIA and the Department of Defense with access to FBI and Treasury Department computer files on 5 million Americans."

Government officials deny the existence of the network. But if the

technology exists, it's hard to believe that the network won't exist soon—if only in the name of efficiency.

One reason implementation will be close to irresistible is that too many of us won't see anything to get alarmed about. Some of us might even welcome the new efficiency.

For instance, I have complained that no physician really knows me. I exist as a series of unconnected parts in the medical files of half a dozen specialists. One knows my insides, another my ears, nose and throat, another my left foot, another my eyes, and so on. Wouldn't it be nice to have one of these specialists assume the role of the general practitioner and put me all together? And if a computer would help him do that, is that so bad?

It would certainly be efficient. Just as it was efficient (until new legislation stopped them) for employers in Washington to send job applicants to police headquarters to obtain copies of their arrest records or a statement that they had none. It would have been even more efficient if the employer's computer could have been hooked up direct with the police department's (and with the former employer's and the government's too, for that matter).

Too much efficiency scares me. I recently had my driver's license renewed, and in place of the old serial number my new license identification is—what else?—my Social Security number. A lot of jurisdictions are going that way, I'm told.

I'm also told that a number of banks are using Social Security numbers to identify bank accounts. It's a safe bet that before long, they'll be using Social Security numbers for credit cards, employee identification numbers, and Lord knows what else, just as they already are doing with military service numbers. Bits and pieces of information. But hear Rowan:

"Setting up a computer network involving virtually any computer, government or private, is almost as easy as making a telephone call. Computers can be hooked together by phone. Once you know the codes for the computers involved, it's simply a matter of dialing in and getting the information you want.

"It doesn't take long. Modern computers copy information at the rate of thousands of pages in less than a second . . . Computers can be hooked together, your records collected in a matter of minutes, then the system can be disconnected, and there's no evidence left behind of what's happened."

And yet, knowing all that, millions of Americans will say: So what? Unless you're a crook, or have done something you're ashamed of, why should you care that computers can talk to each other?

The question presupposes that the information the computers have on us, without our knowledge, is accurate information. That's presupposing a lot.

But even if the data were accurate, clean and posed no threat of loss of reputation, isn't the loss of privacy itself something to get excited about?

[From the Washington Star, July 16, 1975]

Spying Has Come a Long Way Since the Microphone in the Eagle

There is virtually nothing that can't be developed

(By Norman Kempster)

The crowd at a left-wing rally somewhere in South America is rapidly turning into a mob. Suddenly, thousands of people are stricken with stomach cramps and diarrhea. The probability of a riot subsides.

A code clerk in the U.S. Embassy in Moscow types a message on the office electric typewriter. The Russians take down every letter by intercepting the elecronic signals emitted by each key of this—and every other—electric typewriter.

Postal censors somewhere in Eastern Europe open a suspicious letter but discover it is only a routine order for Polish hams. The letter is resealed and delivered to an import-export firm. When the letter arrives, the CIA station—which uses the firm as a cover—brushes the back of the letter with chemicals and a coded message appears.

The super-secret National Security Agency intercepts microwave transmissions of millions of international telephone calls. To have human beings listen in on that many transmissions in an effort to find the one call in several thousand that might be of interest to U.S. intelligence would be an unacceptable waste of highly trained personnel. But a computer is programed to start a tape recorder when certain key words are spoken. The result is a recording of a manageable number of potentially important calls.

The *Glomar Explorer*, the ship with such an elaborate cover story that it aroused worldwide interest in underseas mining, tries, but reportedly fails, to lift a Soviet submarine from the ocean floor.

All of these examples—and uncounted others like them—have occurred in recent years in the shadowy world of spying. They represent technology known to the intelligence agencies of both the United States and the Soviet Union, although supposedly kept secret from the people of both countries.

Spying has come a long way since the 1950s when the Russians hid a microphone in a carving of the Seal of the United States that was presented to the U.S. ambassador and placed in his office in Moscow. The technology includes such exotic devices as laser-beam microphones, filmless cameras and new generation computers.

"There is virtually nothing that can't be developed if you spend an unlimited amount of money," said John Marks, a former intelligence officer for the State Department who now heads the Center for National Security Studies.

A former ranking CIA official remarked, "It is known that the Soviets have a tremendous amount of time and money dedicated to

this sort of thing. This game is played both ways, of course. There is always the realization that if you come up with something really esoteric that you might not be the first to develop it."

The former official, who declined to be identified, remarked that the reality of spying technology is often far removed from the folklore.

"The apocryphal olive that is supposed to transmit from a martini just doesn't work," he said.

No one knows just how much the CIA spends on research and development because the agency's budget is shrouded in secrecy. But government sources say there is no doubt that in addition to its own projects, the agency benefits from technology developed by the Pentagon.

Much of the technological effort is currently being aimed at developing increasingly sophisticated computers.

The far-out research is handled by the Pentagon's Advanced Research Projects Agency (ARPA), a little known bureaucracy which operates at the cutting edge of technology.

In testimony recently to a House Appropriations subcommittee, Agency Director George H. Heilmeier said ARPA's mission was to "focus on the revolutionary rather than the evolutionary."

Heilmeier was intentionally vague in describing the agency's current projects. But he indicated that computer technology was a key element.

"In FY76 (fiscal year 1976, the year that began July 1) we will initate a far-reaching effort on large, high-density computer memories," Heilmeier said. "Although the computer industry is one of the most technically vigorous industries in the country, extrapolation of present industrial trends will not meet our future needs in the area of stimulation, sensor and image data storage, and retrieval related to intelligence data processing. We are breaking new ground to meet the defense needs of the 1990s."

Heilmeier said the agency is engaged in advance research on programs to permit computers to interpret spoken commands.

Heilmeier's predecessor, Dr. Stephen J. Lukasik, provided tantalizing hints of the possible results of such research in his appropriations testimony last year.

"The analysis of electroencephalograph signals has been refined to the point where a computer can discern which of a limited set of commands a user is thinking," Lukasik said. "This research also holds promise of adding a significant new capability to the linkage of man and machine."

Lukasik offered no suggestion of the uses of a machine that could hitch brain waves to a computer. But if perfected beyond the stage that was described to the committee, it could greatly improve the efficiency of a device the CIA uses frequently, the lie detector.

Programming a computer to interpret spoken words has a much more immediate application. Marks said the National Security Agency has computers which can recognize key words like "defense" or "White House" and can even pick out voice prints, the characteristics that identify an individual's speech patterns. The technological capability was confirmed by another source.

The report of the Rockefeller Commission gives a hint of the extent to which NSA intercepts international telephone calls. The com-

mission said the CIA supplied "another agency," the euphemism for the super-secret NSA, with a "watch list" of domestic radicals. The CIA received back "approximately 1,100 pages of materials" related to Operation CHAOS, the CIA's campaign against anti-war groups.

Marks, the former intelligence officer who was coauthor of "CIA and the Cult of Intelligence," said in an interview there can be little doubt that the 1,100 pages of material sent to the CIA represented only a small part of NSA's total interceptions of international telephone traffic.

Much less exotic but equally effective are "harassing agents" employed for crowd-control. Philip Agee, the former CIA operative who wrote "Inside the Company," said these substances include itching powders, powders and gases that close eyes and block lungs, and substances that cause instant diarrhea. He said in a recent interview with Playboy magazine that CIA stations in Latin America use large quantities of the harassing substances.

After several years of wiretapping and bugging scandals, the public is familiar with some of the devices used to intercept and record speech. Less well-known are devices that intercept the characteristic electronic emissions put out by all machines.

Marks said the Soviets intercepted the signals sent off by each key of an electric typewriter in the U.S. Embassy in Moscow several years ago. He said the U.S. has similar technical capabilities.

A former CIA official confirmed that all office equipment puts out a signal. Even photo copying machines "conceivably could be compromised," he said.

In the Playboy interview, Agee said the CIA used a machine which could pick up conversations in a room across the street by bouncing an infrared beam off the window. He said the windowpane picked up vibrations of voices inside the room which were transmitted to the listening station on the infrared beam.

The Technical Services Division (TSD) of the CIA is in charge of handling the gadgetry of espionage. It was this division of the CIA's Clandestine Services that provided White House burgler E. Howard Hunt with the wig and voice alteration device that he inadvertently made famous as the Watergate scandal unfolded.

Other items in TSD's inventory, according to well informed sources, include auto rear-view mirrors that shows the back seat instead of the road behind, lock-picking devices, containers with hidden compartments, equipment for invisible writing, devices for surreptitious opening and resealing of envelopes, telephone taps and similar devices.

Despite the public relations blitz which the CIA has launched to counter recent criticism, the agency refused to discuss gadgetry.

"That comes very close to methods of operation, and that is a no-no," one official said.

"I just want you to know that it was not an ill-fitting red wig, it was a bloody good brown one," the official said.

That was a reference to one of the exploits of Hunt, the former CIA agent and writer of spy novels, who was imprisoned for his part in the Watergate. Acting on orders from then White House aide Charles Colson, Hunt went to visit ITT lobbyist Dita Beard in a Denver hospital.

Mrs. Beard's son later said the visitor was wearing a red wig that didn't fit.

Ever since Hunt testified that he got the wig and the rest of his disguise from the CIA, the agency has been trying to correct what it considers a slur on its technical competence.

TSD also produces documents to establish false identities to protect its officials and agents. Hunt's Watergate exploits lifted the cover on these operations as well.

When Hunt's White House safe was opened after the burglary of the Democartic National headquarters, much of the contents was destroyed. However, federal prosecutors received a complete set of false identity papers that had been used by Hunt and G. Gordon Liddy.

Liddy, under the name of George Frank Leonard, and Hunt, under the name of Edward Joseph Warren, both had drivers' licenses, Social Security cards, policyholder cards from the New York Life Insurance Co. and Continental Insurance Co., and membership cards in the RCA Record Club and the National Rifle Association.

One of the most elaborate technological achievements of CIA research was the *Glomar Explorer* which was used in an attempt to lift a Russian submarine from the ocean floor. To cover the operation, the CIA said the ship was developed by billionaire Howard Hughes to mine minerals from the ocean floor.

To maintain the appearances, Hughes operatives regularly attended seminars on ocean mining. The interest of the Hughes organization in the subject was so intense that other companies became interested in ocean mining, theorizing that if Hughes was involved, there must be money in it.

A recent issue of "Business Week" magazine said Global Marine Corp. participated in the project, although only a few of its employes knew the details of the mission.

The cover was almost blown, the magazine said, when Global Marine's superintendent for drilling inspected the ship and commented on the sophistication of the gear.

"Hey, we could go out and pick up a sunken sub with this ship," he said.

The remark reportedly brought stunned glances from those in the know but they decided to treat it as a joke.

Not everything that pops into the fertile minds of CIA technicians proves to be a success, of course.

One source said the agency developed an aircraft that looked like an eagle and flew like the big bird to confuse enemy radar. The only problem was that—also like an eagle—the craft could only carry about 4 pounds, a payload that severely limited its usefulness.

[From the Washington Star, July 23, 1975]

New Worry: Is the Soviet Listening In?

(Jeremy J. Stone, director of the Federation of American Scientists, was interviewed by Washington Star Staff Writer Orr Kelly)

Question. Over the years, the federation has taken positions opposed to B1 bombers and many new American weapons developments, gen-

erally taking the view that the Soviet Union appears to be less of a military threat than some people in our government think. Now you are talking about how concerned you are about Russians listening in on American telephone conversations. Why this apparent change in your attitude?

Stone. This is not a change in our attitude since our overriding concern has always been national security and freedom in America. In the case of the military weapons programs, we've long believed that the United States had built more strategic weapons than were necessary, which is the general view, I believe, of almost all American citizens—that overkill exists in tremendous quantity. But, in the case of the Soviet Union listening in on our telephone conversations, we see new dangers of manipulation of the stock market, of political forces in this country, possibilities of blackmail. We think more strenuous efforts should and could be taken to prevent it.

Question. How would the Russians go about getting this information and using it?

Answer. For example, you remember the wheat deal in which they were able to outwit and manipulate grain companies. Imagine how much easier it would be if they were able to listen in to the telephone conversations of the wheat dealers preparing their negotiating positions on the prices of the wheat. Or, to take a political example, imagine what the KGB might do if thy decided they wanted to destroy one of their political opponents. For example, Sen. Henry Jackson. They could listen in on his conversations in an effort to find something that would be embarrassing to him. Then it would be an easy matter to leak this to the press.

Question. Do you think it's technically possible for them to sort out, say, one senator's conversations or the conversations regarding wheat shipments?

Answer. Well, we're not sure of this technology because we don't have access to all of the obviously classified information about it. But, we think it stands to reason that this is not so difficult as it might seem. In the first place, it should not be difficult to arrange to listen in to the conversations of any given phone extension, that is phone number.

Question. Would this have to be done through listening to microwaves or can you listen to other kinds of transmissions?

Answer. This would refer to the microwave conversations, but in effect one would sort out the microwave conversations of a given telephone that came over a given telephone number, and one could with computers, we think, further reduce the number of conversations that it was necessary to monitor by having a machine listen for key words in the conversation. There's been considerable talk of this computer possibility in the press in recent days. Since the telephone company itself builds equipment which sorts out all these conversations and directs them to the right telephone line and since all of this equipment is unclassified, all the Russians have to do in effect is rebuild and duplicate the kind of equipment that the telephone compay is using to sort out the conversations. Then they can sort them out themselves.

Question. And, listen to anything they want to listen to?

Answer. That's our impression. In order to verify our understanding of this, we've written to the attorney general to inquire, that is to substantiate our concern, but we've had no answer.

Question. Is it correct that you've asked the attorney general to try to get the FBI to do something about this problem?

Answer. That's right. This is a case in which we think the FBI should be preventing espionage in America.

Question. There have been reports that the government feels that it is not possible to prevent this kind of snooping. Do you think that the Russians' efforts to pick up these conversations could be jammed?

Answer. We don't understand why unnamed spokesmen have asserted that there is absolutely nothing that can be done about preventing the listening in to microwave conversations. In our view, in electronics of this kind, there is always a measure and countermeasure game in which anything that can be listened in to can also be jammed. The jamming can also often be overcome, but then this can also be jammed. So, the question turns on how much effort we are making to prevent this espionage.

Question. Wouldn't the jamming mess up our telephone conversations, too?

Answer. We don't think so. For example, a signal could be beamed at the embassy antenna from nearby the embassy. It would jam the embassy antenna, but not the microwave towers that are transmitting to each other with powerful signals.

Question. Do you suspect that the government might not want to interfere with the Russian operation because we're doing the same thing to them?

Answer. Our speculation is that there may have arisen a tacit agreement between the American intelligence and the Soviet intelligence communities to let each other listen in. This could be called "open telephones," in analogy to the proposal of President Eisenhower for "open skies."

Question. There have been reports in the past that the United States intelligence agencies have been able to listen in, for example, to car radios and official cars in Moscow. That would tend to indicate that we have an interest in using that kind of technology.

Answer. Yes, it would.

Question. Do you have any reason to believe that there is a tacit agreement besides the likelihood that both sides would like to continue this kind of operation?

Answer. Well, the classic tradition of spying and espionage has always been to avoid, if possible, interference with the spies that are uncovered on the other side, but to follow them around, to use them and to manipulate them. This habit may have persuaded our intelligence community to prefer to keep track of Soviet eavesdropping, perhaps to manipulate Soviet eavesdropping rather than to disrupt Soviet eavesdropping. This approach to espionage would be reinforced by the felt American interest in using these techniques themselves and avoiding a jamming war.

Question. How important do you think it is to the United States to get the kind of information that we may be obtaining through this kind of eavesdropping? Would it give us warning of possible attacks and things of great value to the country?

Answer. Happily, our entire strategic posture has long been based on the idea that even a surprise attack without warning could not suc-

ceed because our deterrent would be capable under all circumstances of destroying the Soviet Union in response. So advanced warning is not critical to our security and, indeed, if American plans for counterforce attacks and first strikes prevail, it may be that mistaken indications of advanced warning could lead to preemptive attacks from our side that led to unnecessary escalation in some future conflict.

Question. So you think we would be better off not to have this kind of a warning system because of the dangers in it?

Answer. I think it's unnecessary, and it's significant that the argument in favor of this kind of eavesdropping is not based on the problem of surprise attack but recently has become associated with the felt need for information to verify arms control agreements.

Question. Doesn't that make sense?

Answer. I don't think our arms control agreements should be based on our ability to verify things if that ability is to be easily neutralized or destroyed. In other words, if we reached an agreement for an arms control treaty because we thought we could monitor this treaty with methods like eavesdropping, we might discover a year later that the Russians had interfered with the eavesdropping but that we were stuck with the treaty.

Question. Don't you have a problem, too, in verification that the information you get is not very useful unless you can make it public and tell how you got it?

Answer. I think that's true also. I think that the use of telephone conversations for security matters is not very valuable because there are so many telephone conversations and so little information is contained in them if the other side wants to take precautions and to speak guardedly or to speak in code or to speak over secure lines. If there is a tacit agreement to have an open telephone arrangement, we will trade something very disruptive to our society for something that is not very useful to our society. On the one hand, we would give the Russians an unlimited ability to manipulate and intervene in our society by listening in to things which even in our open society are not open. On the other hand, we will get only the ability to listen into those conversations that the Russians don't take particular care to guard against in a security environment where we don't need advanced warning anyway to protect our security.

Question. Do you think the Russians would really like to have the kind of information they could get from piecing together a lot of telephone calls? Does that fit into their traditions or their interests or their character?

Answer. It's my general impression of Russian history that the Russian secret police for the last 150 years or more have always had a tradition of collecting enormous quantities of information on any foreigner that ventured into the Soviet Union or to what was the earlier period czarist Russia. And, I think that the eavesdropping on American telephone conversations fits very well with Russian style of intelligence.

Question. Do you think there's any danger that the U.S. government in monitoring what the Russians are doing is learning a great deal about secrets of American citizens?

Answer. It has been speculated that the National Security Agency, which is not permitted to listen in on American conversations, is lis-

tening in to them indirectly by monitoring what the Soviet Union is hearing in the conversations it picks up. I think this is possible, and I think that if the CIA asked the National Security Agency for information about American citizens they might get the telephone conversations sent over to them.

Question. Even though they couldn't have gotten this information directly?

Answer. I don't know; it's just a speculation.

[From the Washington Post, July 31, 1975]

'Gun' Mows Down Maryland Speeders

DEVICE ONE OF MANY NEW WEAPONS IN SAFETY ARSENAL

(By Alice Bonner)

A Florida couple driving home from a Maine vacation didn't believe they were speeding yesterday when a brown-uniformed state trooper stepped into the highway and waved them over.

Even more incredible to Clarence and Lois Cantrell was the black, weapon-like instrument held in another officer's hand that had clocked and recorded their 60 mile-an-hour speed—only five miles an hour over the limit—on the Beltway in Greenbelt.

"I didn't think we were going that fast," Cantrell protested as trooper Ray Neigh showed his wife, the driver, figures on the speed gun's digital face.

"That's the first thing they all say," commented Neigh, who had picked off about 60 speeding suspects in four hours yesterday using the new instrument. The radar device is one of several methods, many of them covert, that Maryland state police put into operation this week to crack down on speeders.

State Police Supt. Thomas S. Smith, who announced the enforcement campaign, said that speed limit violators in the state will no longer be warned as troopers carry out Gov. Marvin Mandel's order to cut back traffic deaths and gasoline usage in Maryland.

The 1975 highway death toll stood at 399 yesterday, 30 more than at the same date last year.

From the Van Dusen Bridge high above the Beltway and out of the sight of motorists below, Neigh would aim the radar gun at automobiles below, then radio their speed and description to his partners, obscured by a clump of trees half a mile away, who would stop violators.

"You just aim it and it picks up the speed of the closest car. If you want to clock the speed on (the face of the device), you just pull the trigger," explained Neigh. The instrument can measure the rate of speed from a mile away and with an accuracy within one mile an hour, he said.

Besides the "speed gun" and other "moving radar sets" now in use statewide, motorists might be surprised by troopers in a pick-up loaded with hay, a small foreign sports car, an undistinguished van, or other "normal" vehicles, police spokesman William Clark said.

The disguised speed traps will be unveiled one at a time in a "car of the week" system, police said.

Detection of speeders also could come from overhead. An "eyes in the sky" method, using helicopters over problem areas in conjunction with patrol cars on the ground, will watch for drivers pulling away from the flow of traffic.

For violators, particularly interstate drivers, who tend to accelerate after safely passing a radar set-up, one or more units will be waiting further on.

Not all aspects of the intensified enforcement will be hidden. Regular, unmarked cars with yellow state police tags and marked patrol cars have been authorized to keep their four-way flashers on during normal highway patrolling as reminders of the 55 mile per hour limit.

Another warning measure, the "running roadblock" will employ two or more marked cruisers driving side by side at the speed limit to keep traffic within the legal limit.

"If you use one car, they'll just pass you," Trooper Donald Perkins said yesterday as he and two other officers demonstrated the mobile roadblock.

One problem for which state police have not devised a solution is the use of citizen band radios, mostly by interstate tractor trailer drivers, to warn of speedtraps. Neigh said the truckers nearly all drive "70 or better and there's nothing you can do about it. It's discouraging."

In the first day of stepped-up enforcement, Monday, police reported 930 arrests statewide. They could not explain the high percentage of arrests made in Prince George's County, 287 that day. In Montgomery County the same 24-hour period produced 51 arrests.

[From Newsweek Magazine, Aug. 4, 1975]

True Tales of 'The Other Side'

True, spy tales are few and far between, and Soviet espionage in particular is usually seen only in fragmentary glimpses when a big-time operative is exposed. But in recent weeks, the U.S. intelligence community has been repeatedly hit by exposés of its own illegal activities and troubled by its prospects in a time of détente. As one result, agents have been unusually willing to talk about their rivals' tactics—and Newsweek's *Anthony Marro and Evert Clark pieced together this picture of Soviet intelligence at work in the U.S.:*

In the 1950s, the Russian spy could have come straight from the baggy-pants ranks of Ian Fleming's "SMERSH." But when Anatoli Chebotarev defected to the U.S. in 1971, the company secrets he spilled dispelled what remained of that image. Chebotarev, chief of the Soviet intercept mission in Brussels, told how he had monitored the telephone calls of senior Western diplomats and generals in the North Atlantic Treaty Organization and SHAPE—Supreme Headquarters, Allied Powers in Europe. Whenever a call came in or went out on a key NATO or SHAPE telephone line, Chebotarev said, a computer activated a recorder, which taped the entire conversation. To prove

his boast and entertain his interrogators. Chebotarev mimicked perfectly the voice of a high-ranking U.S. official in Brussels who talked to Washington by phone half a dozen times a day.

Chebotarev's story, U.S. intelligence officials say, typifies modern espionage, Soviet-style. Chebotarev, they note, was an agent not of the infamous KGB but of the lesser-known GRU, a branch of the Soviet armed forces that gathers strategic military, scientific and technological intelligence. The Soviets' ways are infinitely more sophisticated than the cloak-and-dagger methods of the past, and U.S. experts frankly admit that "they're pretty damn good"—in a minority view, "maybe a little better than we are."

Sleepers: Détente, they report, has made it easier for Russia to slip undetected into the U.S. scores of "illegals" or "sleepers"—operatives deposited for several years with false identities, or sent in briefly on one-time missions. There are also 2,000 Soviet-bloc officials in the U.S., sources say, of whom perhaps 800 are full-time "legal" spies (under official cover) and another 800 take on occasional chores. Both legals and illegals have "assets" in cooperative U.S. citizens or resident aliens. In the recent arrest of two men of Armenian descent for espionage, one was an alleged illegal, the other his asset.

These days, the Russians "are sending over young men who are more American than the Americans," intelligence sources say. The young agents are for the first time "flooding the Hill," cultivating Congressional staffers. And they are bringing sophisticated apparatus to feed their hunger for scientific and economic data. Newsweek has learned that the GRU operates at least 48 radio and telephone intercept stations around the world, including four in the U.S., that can monitor private as well as governmental conversations. The Soviet Embassy a few blocks from the White House, the Soviet mission to the United Nations, and the Russians' country retreats sprout clumps of antennas—which, because they are technically on U.S.S.R. territory, are beyond U.S. law. Other Soviet innovations include the "roll-over camera"—a miniature that snaps photographs as it is rolled over a document—and eaves-dropping with laser beams that can decipher conversations inside a room from the vibrations of window panes.

Couth: Has Soviet violence ebbed as technology has advanced? "They've gotten a little more couth," one expert suggests, and many U.S. intelligence sources say that the KGB's notorious Department V, which handled kidnapings and assassinations of foreign political enemies, defectors and obstreperous Soviet citizens, has not been linked to a murder since 1959. But others insist that the Russians have simply become more clever. As evidence of the Soviets' continuing hard line, they point to the KGB's top-secret "watch list"—a 460-page book containing the names, alleged crimes and sentences (death is common) of more than 1,000 enemies of the people.

Most of the best yarns about "the other side" date from the cloak-and-dagger era. One that U.S. agents tell concerns a gray-haired woman whose job was pay-mistress to Soviet operatives in New York. As was common during cold-war days, the FBI kidnaped the woman to a caretaker's cottage on the fringes of a Westchester estate. After three sleepless days and nights of interrogation—perhaps clinched by the reminder that she was near retirement, return to Mother Russia and a pension—she agreed to turn double agent. Agents took her

home, bugged her apartment and listened in from across the street. Six hours later, they heard what sounded like a shot. When no one emerged, they placed an anonymous call to the police—and soon overheard a cop say, "Oh, my God. She's dead. Suicide." More noises, including a dresser drawer being pulled out—and the cop telephoned his precinct that he had found a bundle of cash.

What happened next is disputed. One source says that the money—perhaps as much as $300,000—was delivered to the U.S. Treasury. But others say that the cops were directed by their captain to bundle up the bills and bring them to the station. "The result was that she had a very lonely funeral, and to this day the Russians don't know what happened to their money," says one counterintelligence source. "A couple of cops walked into a major espionage case and looted it and got away."

To indicate the Soviets' almost super-human patience, agents tell about a KGB agent who was discovered not long ago by the CIA in an unnamed Latin American country. After a brutal interrogation by the country's intelligence agents—"They bloody near killed the guy," recalls a counter-intelligence expert—he told his story. It began fifteen years before when as a junior agent he was secreted in a series of Soviet "safe houses" to learn about the Americas and acquire a "legend," or cover story—that he was born in Latin America and reared in a Baltic nation where his family was destroyed—to explain his Slavic-accented Spanish. The agent married a KGB-recruited woman in England and the two were "staged," over the next two years, through three more West European countries.

He bided his time and perfected his legend in Latin America, with two children and a series of small but disastrous business ventures. "He went through $250,000 of the KGB's money," says the expert. But cost was no object, and the agent's lack of business talent didn't count against him. When CIA agents broke into his apartment, they found a congratulatory message with his next destination: the Russian agent's big league, New York.

[From the Washington Star, Aug. 30, 1975]

In Focus—EEG Is Studied as Link Between Man and Machine

from "ship" to "cannon" to "armament"

(By Vernon A. Guidry, Jr.)

Mind monitoring machines to guide a pilot's brain patterns through the cluttered moments of danger or high challenge?

Such a prospect may not seem entirely a Buck Rogers concept to a small agency within the Defense Department which is at work on ways to link the human mind directly to the computer.

The scientist supervising the work has a goal for the program that could mean the ultimate fusion of man and machine: It envisions computers driven by the unspoken thought of the user, and by his very thought processes.

The organization financing the work by private researchers is called ARPA, the acronym for Defense Advanced Research Projects Agency. The thrust of the research is the product of Dr. George Lawrence, a 42-year-old psychologist who has been with ARPA for seven years.

So far, the work has centered on computer recognization of brain wave patterns, or electroencephalograms (EEGs). EEGs, and brain wave research, for that matter, have been around for some time. They are the amplified tracings of the very small electrical currents detectable during brain activity by means of electrodes attached to the head. EEGs are used extensively for medical diagnosis of such ills as brain tumors.

Several studies have been launched to determine the feasibility of putting the art to positive action.

ARPA's first venture began more than three years ago with a contract to Stanford Research Institute to determine whether EEGs had sufficient, consistent information to enable a computer to distinguish one word from another. The question: Could a computer, after recording EEGs associated with spoken repetition of words, identify those words by comparing EEGs when they were later spoken or "thought" by a test subject.

Seven words were employed in the experiment: Up, down, right, left, in, out and stop. Researchers at SRI said they had accurate identification rates of 60 percent to 70 percent. ARPA thinks otherwise. With reservations about methods and the computer used, Lawrence says the judgment is that the study failed to demonstrate an identification rate better than chance. The project was terminated.

"I don't think we can teach the computer to distinguish between words," says Lawrence.

The SRI experiment had envisioned an attempt to reverse the process. If a computer could identify an EEG representing a specific word, could the computer somehow suggest that word to the human mind? Lawrence doesn't know how. "I absolutely can't imagine how it could get information into your head," he says.

More promising is work being sponsored at the University of Illinois. There, says Lawrence, the computer is able to reflect through examination of EEGs the actual information processing going on in the brain. The researchers can watch as a subject's brain grasps a new fact. Research there has also expanded on using EEGs to determine attention levels in subjects.

Within the next two years this research is expected to come up with applications for the cockpits of Air Force planes.

As a general proposition, pilots of combat planes can become very busy. Lawrence suggests that one application of the University of Illinois research could be to determine with a computer whether the pilot is too busy, or busy with the wrong things.

For instance, if one of the plane's warning systems gives an alarm, an on-board computer could determine, by examining the pilot's EEG, whether the alarm had registered. If it hadn't, the system could reinforce its efforts to get the busy man's attention.

Lawrence says current work indicates that the computer might also be able to determine whether the pilot was overloaded, or whether he

was concentrating on one or two things to the exclusion of others—in effect, making an error in judgment.

Another application of the Illinois research could be in computer-aided instruction. The computer would monitor the student's brain activity, tailoring its introduction of new material to the speed at which the student was able to absorb it. The computer, Lawrence suggests, could sense when it should switch from a visual to an auditory presention, when the student needed a break. The computer would thus be providing a completely individualized program of instruction, he says.

In fact, the present state of the art allows the computer to judge the amount of confidence a student has when he picked an answer to a multiple-choice question, Lawrence says.

While he has abandoned attempts to recognize individual words, Lawrence still hopes to be able to "think" to the computer in more or less normal language. Beginning research is now being done to determine whether a program can be devised to enable a computer to infer the general meaning of a word. The program would use a system borrowed from semantics that involves rating words on three separate scales, or dimensions.

The computer would be fed the "locations" of words in these three semantic dimensions. As envisioned, this system could not distinguish between words such as home, house, domicile and abode, but it could infer that each meant about the same thing because of similar locations on the three semantic dimensions and act accordingly.

Lawrence is uncomfortable when asked to discuss how the system might work in practice. "Application is so far away that it would be pure speculation," he says.

Nevertheless, he says it might work something like this:

A user intends to search a computer's memory for information pertaining to, say the armament of ships.

The computer picks up on the word "ships" and begins displaying information, perhaps on a cathode ray tube, about ships, then about cannons on ships. The computer registers the user's mental rejection of cannon and displays more information, in a different area, until it senses that ship missiles hit a responsive note in the mind of the operator.

"Thinking" to computers would work as well for input as for retrieval of information. Lawrence says he is now talking to potential researchers who, among other things, run computer studies of atomic detonations. Their studies involve the complicated process of changing certain factors, such as the distance of the detonation from the ground, to determine how the effects might differ.

Their interest, Lawrence says, stems from the hope that such changes could be made by "thinking" them into the computer.

Such a capability would revolutionize the process of feeding information into computers, an area that is a principal bottleneck in computer use.

It is this kind of revolution that Lawrence is looking for, one that will "bring the computer into a functional role with the human," and make the computer "as responsive as your hand," he says.

The agency backing this research, and other projects ranging from antisubmarine warfare to the high energy laser which it pioneered, is, according to the congressional testimony of its director, Dr. George

H. Heilmeier, a "unique organization" that "tackles the tough, the unique, the unconventional and is not afraid of failure when the prospect of a major payoff in national security is great."

ARPA is housed in one of the Arlington, Va., office buildings that hold some of the Pentagon's overflow. Its corridors are scanned by television cameras and some of its office doors have combination locks instead of keyholes.

For all the apparent security, ARPA's officials are willing to talk about, even patiently explain, their research on people-computer coupling. No aspect of the program is classified, says Dr. F. W. Niedenfuhr of ARPA.

But there are sensitivities involved in the research. Niedenfuhr and Lawrence are intensely concerned that the work might be portrayed as an attempt at mind control. They emphatically insist that it is anything but that.

The point of it all, says Lawrence, is "the enhancement of human performance in Defense Department jobs."

But other questions suggest themselves. If for instance a computer is able to, in effect, eavesdrop on the workings of a student's mind as he answers a multiple-choice question or moves through material being "taught" by the computer, is a question of privacy involved?

Both Niedenfuhr and Lawrence are somewhat surprised by the question.

"We're in a pure research mode and that means only volunteers," says Niedenfuhr, adding that research involving human subjects is now governed by government policy directives. "There's been no apparent danger as far as the thing has come to date."

"No one is going to hold a student down and put electrodes on his head" says Lawrence.

[From the Washington Monthly, December 1975]

The Mind Readers

and other tales of science fiction research by the pentagon's think tank

(By Tad Szulc)

The jet pilot, his flight-suit zipped up, enters a quiet room off his squadron's operations center. Nodding to two white-smocked flight surgeons, he sits in a straight chair that faces a bank of computers. One of the surgeons places electrode plates on his forehead, the other turns on a computer. The pilot is asked questions in a low voice. The computer whirs and feeds out a polygraph tape that registers in curves the pilot's electric brain signals. One of the flight surgeons studies the tape, then shakes his head. "Sorry, Major," he says, "I don't think you should be flying today. Your EEG readout says you're under some kind of stress. Take a day off. Get some rest. We'll read you again tomorrow."

What you have just read is a description of something that, in many variations, may be occurring very soon with some Americans, pilots or not. It is the science of brain waves at work. It is a result

of five years of research by an unnoticed agency of the United States government. The agency is ARPA, a many-splendored—and a bit frightening—military institution.

The initials stand for Advanced Research Projects Agency, and this tiny but vital Defense Department organization, tucked away in an office building across Key Bridge in Rosslyn, quietly functions as a futuristic thinking mechanism with an insatiable curiosity that reaches into the next century and millenium. ARPA's military-oriented technological concepts are so advanced and variegated as to verge on science fiction—except that science fiction in this age is no longer fiction.

Super technology in the realm of computerized communications, handling the flow of military and political intelligence on an unprecedented level of effectiveness, has raised questions among some scientists and others familiar with ARPA's work. Communications computers in a twenty-first century fashion are probably ARPA's strongest point, although this discreet agency also deals extensively with immensely sophisticated weaponry on the ground, in the air, on the sea, in outer space and inner space. The fears, which ARPA officials seek to calm, are that its current research might equip a future American government with a capability for storing and exchanging domestic intelligence on a scale never before dreamed.

That such fears exist, even if they are as unfounded as ARPA claims, is clearly a product of our post-Watergate psychology and the result of recent discoveries about the role of military and intelligence agencies in domestic spying on American citizens. There is, therefore, a nervous reflex in our body politic when it is learned that government agencies are moving toward still new frontiers of intelligence technology. One may be willing today to grant ARPA total credibility—I, for one, am inclined to believe that the Agency's managers are not sinister, minded in a "1984" sense—but the nagging question persists over what happens if, say, a new Richard Nixon reaches the White House.

Still, this is where we must face reality. ARPA is a prime example of the fact that there is no way of arresting or delaying progress—and technology. We may be nervous about what ARPA or some other agency is doing, but research will not be wished away. The way of coping with this dilemma is to look at what is being developed and to hope that, with maximal public knowledge of this research, our political processes can deal with it.

Let us look, then, at ARPA's various and strange activities.

ARPA is working on a computer system that, through the interpretation of electroencephalograph signals, can discern certain command patterns emanating from the human brain. The computer can predict a limited set of human decisions, and it can tell, without a word being uttered by the subject, whether he is seeing red, blue, or yellow. The computer, ARPA says, can operate only with the cooperation of the individual who may wish to let the machine test his strain factors, perceptions, and so on. But the day will come when technology reaches the point where this may be done on an involuntary basis.

All this is not yet quite a mind-reading operation, but it is a giant step in that direction. Scientists say that at this stage it is impossible to define the outer limits of brain-wave technology. In any event,

ARPA says that its research, conducted under contract by several universities, "holds promise of adding a significant new capability to the linkage of man and machine."

Another illustration is ARPA's development of computers responsive to continuous human speech (instead of single command words in systems that already exist), using a 1,000-word English-language vocabulary and, in time, doing away with the traditional keyboard punching by operators. This is man talking to a machine, which thus far responds with 90-percent accuracy.

In terms of purely military research, ARPA's time horizon is "the ten- to thirty-year period." This applies to military technology trends both in the United States and other countries, notably the Soviet Union. In turn, this leads to decisions on the feasibility of ultra-modern weapons and communications systems.

ARPA's concerns range from future tank battles to military underwater environment—submarines are the least vulnerable delivery vehicles in a nuclear conflict and it is vital for the United States to produce literally silent subs while being able to detect movements of Soviet boats. ARPA hopes to come up with a 75 mm tank cannon that can fire 20 times faster than existing weapons (the projection is for two missiles per second), neutralizing Soviet antitank weapons. Lessons drawn from World War II and the Arab-Israeli armor battles have convinced ARPA that the best tank-killer is a super-tank. The Agency's scientists believe that, with the use of highly improved infrared sighting systems, night should become the soldier's friend, not foe.

The catalog of ARPA's ideas seems inexhaustable. There are designs for "packet" transmissions at "burst" speed that, thanks to computer switching devices, can deliver instantaneous messages to any number of military addresees worldwide, breaking through communications logjams.

ARPA has already developed a highly sophisticated network of more than 50 interconnected computers—it is known as ARPANET—that "talk" to each other, providing and exchanging scientific and military data.

ARPA recently advised Congress, "The tactical world will be dominated by systems that are cheap and widely distributed: man-portable anti-tank and anti-aircraft weapons, unmanned remotely piloted vehicles, and unattended ground sensors directly coupled to weapon systems." What ARPA is talking about, then, is the automated battlefield of the future, heavily dependent on lasers and other guidance methods.

In the past ARPA has dabbled in a scientific approach to counter-insurgency, probably one of its least successful efforts. It was known as Project AGILE. ARPA laboriously produced English and Vietnamese-language handbooks on counter-insurgency, but clearly this project failed to alter the course of history. Likewise, ARPA conducted military feasibility studies on the use of defoliants in Vietnam, finding them highly promising. But again, defoliation, while disfiguring the Vietnamese countryside, was never an effective weapon. The Defense Department denies that around 1960 ARPA was involved in studies on lethal and traceless shellfish toxins (the assassination poisons that were not destroyed in 1970 in violation of a White House

order). The allegation by former officials attached to ARPA was that it had worked on toxins on behalf of the Central Intelligence Agency's Technological Services Division and the U.S. Army.

ARPA's basic philosophy was summed up recently by its young, scientifically gung-ho director, Dr. George H. Heilmeier, who last year, at 38, received the Outstanding Young Man in Government award. Heilmeier said: "We guard against technological surprise."

ARPA owes its existence to the fact that the United States was technologically surprised in 1957, when the Soviet Union launched its first Sputnik satellite. Former President Eisenhower's immediate reaction to Sputnik was to turn to the Army, Navy, and Air Force to request their advice on how best the United States could come up with a satellite of its own. As the story goes, Eisenhower received three differing sets of responses from the services, and he finally concluded that the Pentagon had to create a centralized technological research capability.

The result was the creation of ARPA early in 1958—and, in short, the design for the first American earth satellite. ARPA became a separate agency in the Defense Department, operating directly under the control of the Secretary of Defense and thus enjoying an almost unparalleled autonomy for an agency of such small size. ARPA currently employs 55 scientists, most of them with one or more advanced academic degrees, and 115 support personnel; by Washington bureaucratic standards, the Agency is a virtual Lilliput, but a Lilliput with clout. As Dr. Heilmeier put it in recent Congressional testimony, "We report to the top of the chain, not the middle." ARPA's only bureaucratic link in the Pentagon is the Director of Defense Research and Engineering, an office on the Assistant Secretary of Defense level, providing the Agency with staff supervision. Dr. Heilmeier himself served for nearly four years as an Assistant Director of Research and Engineering before former Defense Secretary James R. Schlesinger picked him last March to take over ARPA.

A plain-talking, no-nonsense Pennsylvanian with a Princeton PhD in solid state electronics, Dr. Heilmeier sees ARPA as unique in its freedom. He is clearly enamored of ARPA's "revolutionary" approach to defense technology, but he is not Dr. Strangelovish about it. He is too relaxed and matter-of-fact about his work to fit the cliché image of the power-mad scientist, and he is free of the distortions and insecurities of the typical Washington top-level bureaucrat. He makes no bones about his pride in ARPA. This is how he described his Agency to the House Appropriations Committee:

"ARPA is a unique organization with a unique role. . . . [It] tackles the tough, the unique, the unconventional and is not afraid of failure when the prospect of a major payoff in national security is great. . . . It focuses on the revolutionary rather than the evolutionary. . . . It has the freedom to take alternative paths that run counter to popular beliefs or widely held opinions in order to provide decision makers with a set of alternative opinions. . . . It has no vested interest in the status quo. . . . Our research is for the breakthrough, the elegantly cheap, the simple, the effective technical solution. These may be very different from traditional approaches. . . . There will be failures. . . . As Director, I believe that I can guarantee

to you that the bottom line will show a clear gain in future national security . . . a fair return for the public investment."

Considering what ARPA does in its many fields of endeavor, it is "elegantly cheap" to the taxpayer. For fiscal year 1976, Dr. Heilmeier asked Congress for $226 million, a 12-percent increase over the previous year. This is roughly one-quarter of one percent of the total defense budget this year. But Heilmeier's notion, following that of his predecessors, is that by staying clear of the bureaucracy there can be immense return on a small investment.

Thus ARPA farms out all its research to outside scientists and universities. There is no laboratory on the three floors ARPA occupies at 1400 Wilson Boulevard; the 55 scientists working there are essentially project manager for outside ARPA research, and, as Heilmeier points out, few of them stay more than five years at the Agency—presumably to be spared the temptation of developing vested interests in projects they manage.

While ARPA funds the outside research from its appropriations, actual contracts are negotiated and written by the Army, Navy, or Air Force, again to keep the Agency free of bureaucracy. Some ARPA watchers claim that it also funds research for the CIA through a system of reimbursement, but the Agency cannot ever be identified with it because of the contract-writing method. ARPA officials deny any knowledge of assisting CIA research.

Heilmeier is probably right in his claim that "ARPA draws on the most creative talent in industry, universities, and government" and that "because of its stature and reputation in the technical community, the most imaginative scientists and engineers in the country seek out ARPA's support." He explains it by saying that these scientists and engineers know that at ARPA they will face "a minimum of bureaucratic uncertainties, tough, knowledgeable questioning of their ideas, an awareness of the intrinsic value of their work and its application to national security even though they themselves may be unaware of its total impact, a willingness to take technical risks when the payoffs are high."

As matters now stand, scientists from the Massachusetts Institute of Technology to the University of California and a dozen other famous schools are involved in ARPA research. Some of these scientists belong to a highly exclusive, informal group known as the "Golden Fleece," men and women picked in the late 1950s by the Pentagon-funded Institute for Defense Analysis for some of the most esoteric and complex defense research. ARPA, upon its birth in 1958, immediately received the benefit of the talents of these "Jasons," as they are still called. ARPA officials says that some 20 "Jasons"—an elite, informal, almost secret group—are still at its disposal. Over the years, the "Jasons" have been holding quiet brainstorming sessions at hideaways around the country to feed ARPA ideas.

As a rule, ARPA moves away from a project once it has been completed, turning it over to the appropriate military service for further engineering and use. A possible exception is the ARPANET, the super-computer network.

ARPANET's most important computer is the $40-million ILLIAC IV at the Ames Research Center of the National Aeronautics and Space Administration (NASA) at Mountain View in California.

ILLIAC IV is the king of American computers, capable of more complex operations than probably any single computer in the world. It includes a dozen terminals at military installations in the United States and at least four overseas. Universities and several computer corporations, such as UNIVAC, are part of ARPANET.

ARPA itself maintains offices in Honolulu and in West Germany, but ARPANET computers abroad are located at the University of London and at Kjeller, Norway, the site of the Norwegian Seismic Array headquarters. ARPA explains that the Norwegian terminal is related to the United States program of seismic detection of underground nuclear explosions; it is near enough the Soviet Union to pick up seismic signals of Soviet tests. Seismic detection is one of the most important ARPA projects, particularly in terms of the recent Soviet-American agreement of maintaining underground nuclear testing below a certain threshold of power. ARPA's equally strong interest in undersea acoustics—the propagation of sounds emitted by submerged submarines—is also served indirectly by its seismic research. The agency is involved in studies of Soviet satellites too. Recently ARPA helped to install a top secret satellite-monitoring station in Australia.

The most significant thing about ARPANET is that it permits the instant connection of computers of different types, ranging from the huge ILLIAC IV to the commercial-class models produced by IBM and others. Complex switching techniques allowing these computers to "talk to each other" are considered a major technological breakthrough. The question that goes on haunting civil libertarians is whether ARPANET can be used for domestic intelligence by being hooked into CIA, FBI, military intelligence, White House, or other computer systems.

ARPA officials go to great pains to explain that it is neither necessary nor practical to turn to ARPANET for domestic intelligence activities. The same point was made by officials in the intelligence community who pointed out that the White House, the FBI, the CIA, and the military agencies had perfectly adequate computer systems to deal with domestic intelligence—if this is what they wish to do. The Defense Intelligence Agency, for example, recently requested new funds from Congress to complete a new computer communications' system to link the National Military Command Center at the Pentagon with the National Military Intelligence Center, the hub of all military intelligence in the United States. As is widely known, the Army used its intelligence resources in the late 1960s and the early 1970s to collect and store data on American citizens allegedly engaged in antiwar or radical activities. It cannot be ruled out that the Army will not do it again, despite Congressional strictures, nor that the DIA's new system will not be used for it. After all, the National Military Command Center—supported by the National Military Intelligence Center—has the responsibility, under a series of Pentagon directives, for the control of civil disturbances.

There is no evidence, however, that ARPANET has been devised with domestic intelligence in mind. ARPA officials say that the network has never been employed for anything except the computerized exchange of military scientific data among the institutions forming ARPANET.

Still, the question lingers: Could the next Nixon order ARPANET to be turned into a police instrument, instantly telling every government agency everything there is to be known about every American citizen whose name has been recorded somewhere?

And if ARPANET has the capability of telling all about what Americans do and say, does ARPA have the possibility of telling what Americans *think*?

The qualified answer is yes. ARPA says, "The analysis of electroencephalograph signals has been refined to the point where a computer can discern which of a limited set of commands a user is thinking."

Scientists working on the project at several universities (which are linked by ARPANET) explain that new research has proved that brain signals have a meaning that can be interpreted by a computer. The research centers on devising a "language" that would translate brain signals into an understandable vocabulary.

There are, of course, limits on mind reading by computers. Dr. Emmanuel Donchin of the University of Illinois, one of the scientists engaged in brain-wave studies under ARPA auspices, says that the computer can establish whether a decision has been made by the human brain, but not *what* decision.

Dr. Donchin and other scientists interviewed for this article say that thus far their research is concentrated on the interpretation of the brain's electric signals from which it is possible to infer what people may do under certain stimuli. The process, scientists say, is "noninvasive" in that it is conducted with the cooperation of the individual to whose skull electrode terminals are attached for an electroencephalographic read out. Under questioning, several scientists acknowledged that there is nothing to prevent an "invasive" experiment with, say, a war prisoner.

Here are some examples of how computer mind-reading can work now:

If electrodes are attached to the skull of a jet pilot or astronaut, scientists on the ground can monitor how he is allocating his attention among the increasingly complex tasks he faces in the cockpit.

Reading of brain waves before take-off can establish whether a pilot is mentally capable of going through the preflight check list. Likewise, a computer can determine whether a pilot is suffering excessive stress that may interfere with his optimum performance.

EEG readouts can tell whether a radar operator has exceeded the stress limit from concentrating for too many hours on the movement of blips on his scope. ARPA scientists say that such knowledge derived may be critical in a moment of national emergency, such as enemy preparations for a nuclear attack.

Brain signals, properly interpreted, can tell whether a student is absorbing the lesson he is learning. This can be expanded to all aspects of intellectual perception and retention.

Flashing different colors at a human eye produces brain responses that the computer can extract from brainwaves and identify according to the actual color. The brain emits a recognition pattern of colors that the computer can interpret. Thus far, the computer can deal with only three colors.

The computer can determine whether the brain is reacting to an expected or non-expected stimulant. In plain words, it means that the

computer can tell whether the subject has been surprised by an experience to which his brain has been submitted.

Scientists say that there now is an outer limit to this type of brain-reading research, but that theoretically there may be no real limits. One scientist noted, "You're dealing with ten billion cells in the brain, each with 10,000 connections with other cells—so how can you really determine what is possible? Each day we're learning something new in brainwave science."

Another of ARPA's most interesting challenges is how to cope with the mass of information increasingly reaching military computers. The point has already been reached where computer communications channels can no longer absorb and retrieve logistics, command, control, and intelligence data that is being fed in from all sides. Thus, ARPA says, "it is necessary to . . . discover new technological bases for computer memories that will make it possible by the 1990s to store and process thousands of times as much information as can be handled by present-day computers."

To simplify the handling of computer data, ARPA is involved in advanced research on the use of human speech to activate the machines. This is known as the "speech understanding program," and Dr. Heilmeier hopes that a "final concept demonstration" can be made next year.

The idea of speaking to computers is not new. Even today, computers at post offices around the country automatically sort out mail when a zip code number is spoken into a microphone. This is known as a "discrete" command with the computer programmed, rather simply, to respond to single-word commands. But, as Dr. Heilmeier sees it, the quantum jump in ARPA's research was the transition from "discrete" signals to continuous English speech, which need not be formed in pre-arranged sentences.

As he explains it, ARPA is mapping "speech wave patterns into symbolic representations usable by computers." Intellectually, this is one of the most fascinating areas of modern research in which the computer science is wedded to linguistics' concepts.

The first step in this process is to transform acoustic forms—English sounds—into phonemics. A phoneme, according to Webster's unabridged dictionary, is "a group of variants of a speech sound, usually all spelled with the same or equivalent letter and commonly regarded as the same sound, but varying somewhat with the same speaker according to different phonetic conditions," such as "neighboring sounds, stress, length, intonation, and so forth." For example, the "l" sounds in leave, feel. truly, and solely, though, acoustically different, belong to the same phoneme, since their variations are due to phonetic environment. ARPA researchers have concluded that approximately 40 phonemic symbols can represent English speech "without information loss." This transformation is accomplished by the computer.

The next step is to transform phonemic symbols to orthographic symbols, in other words to the 26 characters in the English alphabet. This, too, is done instantaneously by computer. The machine cannot handle English sounds, but it can cope with letters of the alphabet. Existing speech-recognition systems require the insertion of deliberate pauses between words—a standard computer absorbs a word at a time—but, according to Dr. Heilmeier, ARPA's great success was to develop a

continuous-speech process. The computer has to be addressed slowly, the way one speaks to a child, roughly at one-tenth of the human speaking rate, but the speaker can use up to 1,000 words in the English vocabulary.

This system speeds up the programming and retrieval process. It also frees the hands of the user if, for example, he is a pilot addressing a cockpit computer—but the man and the machine must be literally acquainted with each other. A computer of this kind is programmed for average American English; because of the phonemic requirements of this process, the whole operation can break down if the computer is unexpectedly addressed in the Southern accent by, say, a pilot from Alabama, or in the German accent by Secretary of State Henry Kissinger, should he acquire such a machine to help him run foreign policy. In such a case, the computer has to be programmed for the Harvard variant of the German accent.

Finally, ARPA's primary responsibility is to conduct advanced research for the development of better and smarter American weapons. The Agency is equally concerned with Soviet research in such refined fields as electron beams that have an application in weaponry, high resolution radar, and space communications. This is where the Soviet technology, according to ARPA, is at its best.

Dr. Heilmeier's scientists also conduct war-gaming for the Pentagon's benefit, trying to assess, for instance, the impact of Soviet-Chinese rivalry on United States defense forces. They have completed a model of the Soviet economy to determine scientifically how Moscow is dependent on foreign trade and technology both in normal times and in crisis situations. ARPA worries about low-intensity conflict situations around the world—for example, the problem of the Spanish Sahara—and what it calls "non-standard wars," a euphemism for guerrilla warfare.

As Dr. Heilmeier sees it, ARPA is an investment bank for the Defense Department's technological needs. His role, he says, is "investment decision-making"—to see what pays off and what doesn't, in terms of America's technological defense needs in the far future. In the last 17 years, he believes, ARPA's investments have paid off in an extraordinary manner. It is hard to argue with science fiction that suddenly becomes a palpable reality, and this is what makes tiny ARPA such an important star in the Washington power constellation.

[From the Washington Star, Feb. 23, 1976]

Are Computer Hookups to the Brain Next?

THE ULTIMATE IN TECHNOLOGY PREDICTED

(By Cristine Russell)

Boston.—Implantation of direct hookups in the human brain may be the "ultimate computer technology of the future," a Rockefeller University scientist predicts.

Such a prospect, dependent upon progress in "breaking the internal codes of the human mind," might be possible in as little as 20 years or may take "several decades more," according to Dr. Adam V. Reed.

But the 30-year-old experimental psychologist, who was earlier trained as an electrical engineer, expects to see "electronic extensions" of the brain within his own lifetime.

His futuristic speculation was part of a symposium on "Man-Computer Relations" yesterday at the American Association for the Advancement of Science meeting here.

Reed acknowledged the need to protect against the dangerous applications of "thought control"—turning human beings into virtual robots—but his emphasis was on what he saw as the potential benefits.

"As an aid to thought, it should be capable of implementing these processes with improved speed and reliability.

"As an aid to memory, it should provide the user with an almost infinite data capacity," he said.

Implanted under the scalp, a user's terminal, and preferably an entire computer, could "cease to be an external, conscientiously manipulated artifact, and become no different, from the user's viewpoint, from any natural part of his brain," said Reed. Whenever a person wanted to know something it could be right there in his head.

"This would eliminate distinctions between experts in individual fields and individuals," he suggested. Instead of relying on a surgeon to make a decision for him, for example, a patient at a hospital could decide whether a given operation was really necessary.

Is this a pipe dream or a real possibility?

Other computer experts on the association panel took a more conservative view as to whether human computer hookups were likely to happen or even whether they could ever happen.

"It will probably take 20 years to learn if it's possible," said William A. Woods, a senior scientist at Bolt Beranek and Newman, Inc., in Cambridge, Mass.

Reed agreed that the "science still hasn't been completed," but he cited some leads he views as promising.

Connecting brain cells with the computer "will require only a qualitative improvement of currently available unit recording technology," said Reed.

He noted that thin wire micro-electrodes are already routinely used in animal experiments. And with the trend toward minaturization, he feels that micro-electrodes one-tenth as thick as those now available could be developed so that one hundred thousand could be contained in an area less than one-twenty-fifth of a square inch.

There has also been some progress in moving in the other direction—taking information from the computer and putting it into the brain. Experiments are now being conducted with electronic devices for the blind, which feed visual information into the surface of the brain, said Reed.

But the difficult problem of locating individual cells in the brain for the computer hookups remains.

The main limit, however, is the difficulty of unraveling the internal language of the brain. This is where advancement is likely to be painfully slow.

Despite the futuristic and unpredictable timetable of attempts to mate man's mind with computers, Reed said, "he was bringing it up now so we would have time to think about the implications of such technology."

"I think there will necessarily be intermediate steps before people would even want direct hookups," said Dr. John McCarthy of Stanford University's department of computer sciences.

Closest at hand, he suggested, is the home information terminal, connected by telephone to a computer which has access to a worldwide variety of materials, from the latest book to up-to-date airline schedules.

"Within the next 20 years and beginning within the next five, the home computer terminal will revolutionize the way we conduct our personal business as much as the automobile revolutionized the ways we get around," said McCarthy.

"The technology for information utilities serving home computer terminals is already here," he said, but "the organizational problems of creating new public utilities are formidable."

[From the Washington Star, Aug. 4, 1975]

Stress Evaluator Reporting—Is It Journalism or Mere Gadgetry?

IT COULD MAKE THE FOURTH ESTATE AN UNCHECKED ARBITER

(By Alan Frank)

Separating fiction from fact remains a highly unscientific if often genuinely exciting occupation for millions of law enforcement, medical, journalistic and other reputable and respected tradesmen across the planet.

Traditionally, the process has been dominated by a carefully structured but largely instinctive blending of accumulated knowledge and gut-felt vibrations: the wavering glance, the misplaced date, the damp palm, the mini-contradiction.

But science, being what it is, has been moved into the situation in a manner praised by its defenders and assaulted by its victims and the cautious and concerned. The first and heretofore most controversial example is the conventional lie detector or polygraph machine, an apparatus increasingly used in commercial and often legal affairs. But the cumbersome and cooperation-demanding machine has left even its proponents desirous of a more remote and facile invention.

Some feel they have found such a device in the PSE, the Psychological Stress Evaluator, which reputedly can discern truth from the shake of a person's voice.

Spurred by endless fascination and nearly endless marketability of the intricate mysteries of stories about the Kennedy family, several publications have begun employing former intelligence officers as PSE-equipped journalists.

This new breed of reporter orients his logic around the PSE verdict about his subject's voice patterns. Pencil and paper reporting is

strictly secondary and wooing secretaries for tidbits of information is oldtime newspaper movie romanticism.

The only trick is to get the conversation on tape. There is no informed sources nonsense, no problem securing secret documents.

The old methods of dealing with tricky stories have failed to produce the truth about John F. Kennedy at Dallas and Teddy Kennedy at Chappaquiddick, the intelligence officers cum journalists say, so they want to give their PSE machines a workout.

In the National Enquirer, Penthouse and other publications, stories proclaim the PSE can prove assertions of innocence and often make clear guilt that had once been rife with hush-hush innuendo.

Perhaps more important than the efficacy of the current spate of lie detector-based stories is the impact the PSE could have if it becomes standard equipment for reporters.

Reporters who currently examine records, record and interpret statements by politicians and others, then present written accounts of the events without making judgments of truth or falsehood would find their roles as translators of happening radically changed.

If the PSE works as well as its supporters claim, using the machine could make the Fourth Estate an unchecked arbiter of all public statements.

The beauty and beast aspects of the PSE are indivisible. The machine requires only an audible tape of a human voice to perform. Unlike the polygraph test, with its requirement of consent from the person who must be wired into a special chairlike contraption to be tested, the PSE can be run without permission from anyone.

A tape recording of a broadcast press conference, a taped telephone call, a transmission from a surreptiously bugged room, almost anything that can be recorded, can be subjected to the unblinking machine. It spews forth a two inch wide strip of graph paper with marks indicating an individual's stress levels.

Its inventors, Alan D. Bell and the other officers of Dektor Counterintelligence and Security, Inc., of Springfield, Va., claim that the machine is intended to be used as a replacement for the lie detector in law enforcement and security work. Bell clearly is proud, not dismayed, that his machines, run by people trained by him, also are being used for journalistic endeavors.

Several television stations, tabloids and even the U.S. News and World Report have used the PSE, particularly for journalistic replays of testimony by Watergate figures John Dean, John Mitchell and Richard M. Nixon.

Dektor Vice President Charles R. (Bob) McQuiston is the latest of the PSE journalists. The National Enquirer recently hired him to analyze Sen. Ted Kennedy's taped July 1969 press conference about his role in the accidential drowning of Mary Jo Kopechne at Chappaquiddick.

The Verdict: "EXCLUSIVE—Scientific Evidence Proves: Ted told the truth about Chappaquiddick."

In a story written by Enquirer Associate Editor William Dick, ex-Army intelligence officer McQuiston said, "By using the PSE equipment, I've been able to take a trip few men can duplicate—a trip through the mind and personality of Ted Kennedy. . . . As it now

stands, I know a great deal more about Teddy that he doesn't know I know."

George O'Toole, formerly in charge of computer bank at the CIA's Problem Analysis branch and now a "freelance" writer, is the most ambitious of the PSE journalists. He has written a Penthouse-sponsored book called "The Assassination Tapes" which declares that Lee Harvey Oswald did not shoot John F. Kennedy and that the Warren Commission investigation needs to be reopened.

The book outlines O'Toole's modus operandi in lining up people to interview in Dallas about the assassination: "In the guise of a magazine journalist writing a harmless commemorative piece . . . he sought them out. He took along the tape recorder."

The tapes capture and the PSE evaluates microtremors of the voice, vibrations ranging from 8 to 14 cycles per second which are undetectable by the unassisted ear. The microtremors, Bell said, are uncontrollable, by even the most skillful orator and can be broken down in 32 ways by the machine.

"What it really does is it highlights the areas that should be investigated. You can be very confident, in some circumstances, that somebody is telling the truth," said O'Toole. "You can not be equally confident in an unstructured interview that you know someone is lying, but you at least know that you have touched on a subject which has caused the person to experience a great deal of stress, which may be due to deception.

"Unless you understand why a person stressed on the subject, there is obviously an important part of the story you don't understand. It identifies areas that should be further investigated by more conventional means."

O'Toole and Bell believe that once the value of the PSE as an investigative tool "sinks in," more writers will begin using it.

"I haven't seen it being used by many other journalists," said O'Toole. "Part of the problem is that most writers have backgrounds that don't really encourage them to use something like this."

Bell added: "Most journalistic endeavors are slap-bam-bang, 'Let's grab the cream off the top and go.' What most journalists would like to see with this is an instant red light-green light. Is it the truth? Is it a lie? In other words, they would like to see some magic. We try to dissuade them from this whenever possible."

"Most stories are written against a fairly short deadline and don't necessarily go into a depth of investigation that even makes it perhaps worthwhile to use this sort of approach."

"There are very clear limitations to the process. The limitations basically are in the human being," Bell said. "If I were allowed to go back and redesign the human being, I could smooth a lot of these things out. But we are limited to human psychological reaction."

"What we are looking at is not truth or lying in the philosophical sense: we're looking at reaction or lack of reaction," said Bell. "If he lies, there will be a reaction. Therefore if there is no reaction, he has not lied. But if he reacts, even though it could be because of his lying, it is not necessarily. He may conceivably be so emotional to the subject matter that he may react."

Bell claims he has some scruples, some standards about the journalistic uses of his machine. "There was one of our users that did some

stuff on the Patty Hearst tapes. We weren't too damn happy about this. We got hit on doing this and refused to do it because while Mitchell and Dean were in a position to defend themselves, we weren't really sure that Patty Hearst was. We didn't see what favorable purposes this would fulfill that would be offset by the unfavorable possible reaction."

To some mainline journalistic scholars, such as Fred W. Friendly, Edward R. Murrow professor at the Columbia University Graduate School of Journalism, the PSE is little better than witchcraft.

"It sounds like nonsense to me. As somebody who has worked with the voices of great men and charlatans all his life, that anyone who thinks that he can divine or determine who's telling the truth and who isn't by the sound of his voice or the quality of his voice is kidding himself," said Friendly.

"Some of the worst charlatans have always sounded as if God and country were on their side and some of the most devout and loyal patriots often sounded as if they weren't telling the truth because of just the psychological nature of their ability to face an audience or an interviewer," said Friendly.

"If you listen to some Murrow tapes, you'll find his voice cracking, even though this was the most consummate professional broadcaster there ever was. Part of his intensity was that sometime his voice would crack and show emotion," said Friendly. "On the other side, people like (Joe) McCarthy and McCarran were able to maintain perfect tone or pitch that had nothing to do with truth or falsehood."

Friendly believes it would be "disastrous" for journalists to begin using lie detectors of any variety. "I don't think it's a journalist's job to tell truth or falsehood from the sound of a man's voice or even a lie detector machine. If law enforcement people want to do it, that's one thing, but it is not our job to be a jury, to say this man is telling the truth or this man is lying.

"It's our job to present all the facts and all the undertones and overtones and let the reader and the viewer make up his own mind. Journalism is not an arena for the gadget. It's a place for hard work, no tricks. When we start using a gadget like that, we might as well stop being a journalist and start being magicians."

The influence of the PSE, whether it becomes acceptable to newsmen from major newspapers and broadcast companies, is undeniable.

During a recent televised interview with former Warren Commission member John McCloy, CBS commentator Eric Sevareid based a question about the quality of the commission's investigation on information contained in O'Toole's book, "The Assassination Tapes."

"I'd hate to have my fate placed in a gadget like that," Sevareid said later. He also dismissed possible use of the PSE as a reporting tool. "I hope we don't come to that point, frankly. It all sounds a little esoteric to me. People have too much awe about computers and gadgets. I wouldn't be very enthusiastic about that kind of journalism. We don't know enough about human psychology. This is maybe the last of the sciences, the human brain trying to understand the human brain. I would think it is all extremely fallible and tenuous. That's just my horseback reaction."

National Enquirer Associate Editor William Dick, who has used the PSE, believes critics of the machine are short-sighted.

"We read a lot about the PSE and we thought it (the Ted Kennedy story) was a pretty interesting thing to do. I can see a pretty wide use of the PSE in journalism," said Dick. "For instance, if a politician stands up and makes a controversial statement—such as the Ted Kennedy thing, which wasn't political—I could see it being used."

"Now, it doesn't tell you whether a guy is lying, but it does tell you whether he is telling the truth," added Dick. "From the tests we have run on it, I believe the machine. Not that it is a lie detector but it does tell you if the guy is telling the truth."

"I don't think it's witchcraft at all," he said. "It is a scientific machine which can aid us in assessing what is the truth, I believe. We will be using the PSE on several other tapes." Dick said the PSE "certainly will be" a tool in the repetoire of National Enquirer reporters.

Another newsman whose paper has used the polygraph as part of a story believes the lie detectors have no role in reporting. At the Philadelphia Daily News, where Philadelphia Mayor Frank L. Rizzo and Peter J. Camiel, a political opponent of the mayor's, once subjected themselves to lie detector tests, the editor disapproves of the use of lie detectors.

Rolfe Neill, editor of the News, said his paper stands by its headline that declared "Rizzo Lied" after the mayor flunked the polygraph test. But Neill does not consider the polygraph or the PSE as journalistic tools. He said both Rizzo and Camiel volunteered to take the test and the newspaper acted only as a willing intermediary in sponsoring the polygraph.

Asked what place the machines have in journalism, Neill said, "In my opinion, none. Still the best check for journalism is just the digging that is involved in good reporting.

"You certainly are not going to catch all the crooks in the absence of secret listening devices and lie detectors and so forth, but it seems to me that society has been well-served when its journalists have been of the right caliber," he said. "And they were not armed with lie detectors nor Psychological Stress Evaluators. There's a certain circus atmosphere that is inevitable with such mechanical measurements."

"We've always been careful to point out that it was not our idea. It was Pete Camiel's idea and what really made it a fine story was that the mayor lied," Neill said. "I don't think that that's the way to conduct government or newspaper offices or any thing else, by lie detector."

"As a matter of public policy, I don't think so," said Neill, "but if two fellows want to hook themselves up to a polygraph, sure, we'd be happy to supply the examiner."

[The Washington Post, Nov. 7, 1976]

The GOP "Lie Detector"

(By Morton Mintz)

The Ford campaign used a controversial machine called a "voice stress analyzer" to try to audit Jimmy Carter's truthfulness in the first two presidential debates, a Republican National Committee official said yesterday.

In the process, the machine's manufacturer told a reporter, he found that President Ford's voice registered "heavy stress" each time he mentioned the word "Congress."

For undisclosed reasons, the President Ford Committee chose not to publicize the result of either the Carter or the Ford analysis. "Obviously, whatever they found in those recordings was not used," said Peter B. Teeley, a Ford committee spokesman.

Eddie Mahe Jr., executive director of the Republican National Committee, said that he and Stuart Spencer, Ford's deputy campaign director, were reluctant to publicize the Carter result because "this was the kind of thing that can whip around on you and blow up on you 14 ways from Sunday."

The maker of the device, Rick Bennett of the Seattle suburb of Issaquah, said he had hoped to have the Carter result publicized before the election, claiming it would have changed the outcome.

But he refused to detail the finding yesterday, saying that in the post-election period, 51 per cent of the voters—those who voted for Carter—have "a vested interest" in him, and that disclosure might lead to ruination of his (Bennett's) fledgling manufacturing enterprise, called Hagoth Corp.

Asked why Ford showed heavy stress whenever he mentioned the word "Congress" during the Sept. 23 and Oct. 6 debates, Bennett said he believed the President's tension reflected the difficulty of dealing with a House and a Senate dominated by Democrats. For that reason, he said, he urged publicizing the finding.

Spencer feared, however, that voters would view Ford's stress as meaning that if elected he could not work with a Congress certain to remain Democratic and for that reason preferred silence, Bennett said in a telephone interview.

If the Ford campaign had claimed that the machine impugned Carter's truthfulness or verified Ford's, questions about the voice analysis technique might have been raised.

Voice analyzers are supposed to measure giveaway modulations in the human voice when a lie is told. By 1974, more than 500 of the machines were being used by police agencies and private organizations here and abroad. The principal producer was Dektor Counterintelligence & Security Inc. of Springfield, Va.

The Army, which owned three of the devices, had a study made by a Fordham University psychologist. In a report in February, 1974, the Army said the study indicated a "clear inferiority of voice analysis . . . not only to the polygraph but also to judgments made on the basis of simply observing subjects' behavior.

Last year, New York writer George O'Toole, who used electronic equipment to make analyses for the Central Intelligence Agency for three years, claimed that his tests with a voice stress analyzer showed that Lee Harvey Oswald had told the truth when he claimed he had not killed President Kennedy.

Bennett said the devices are "very reliable." One "proof," he said, was in his six months in business he has sold more than 50 of them with an unconditional guarantee of a refund of the $1,500 purchase price and no one has asked for a refund.

The Washington connection began last month when Roger McLoughlin of Denver, a vice president of Bennett's firm, told a former

Ford aide that Bennett had monitored Carter's voice and had gotten "damning information."

As the Republican committee's Mahe tells it, McLoughlin contacted him to offer to do an analysis, free of charge, of stress registered in tape recordings of Carter's voice in the first two debates. "McLoughlin was particularly aggressive, wanting to get exposure and to get to the press," Mahe said.

The upshot was that on Oct. 20, McLoughlin and Bennett demonstrated the machine in Spencer's office, and then, at the RNC, spent about 12 hours reviewing debate tapes. They underlined sections of the transcript where the needle on the machine swung, purportedly showing Carter to be under stress.

The next day—the eve of the final debate Oct. 22—Mahe sent the underlined transcript to Spencer. The response of the Ford campaign official was silence. The needle didn't move.

He recalled being skeptical, saying it wouldn't surprise him if stress showed in men whose "goals, ambitions, dreams" rode on their performance in the debates. But it "sure as hell wasn't my business to make the decision," he said, so he put the matter before Spencer.

[From Newsweek, Sept. 8, 1975]

"No Place To Hide"

When the Rockefeller commission reported on CIA surveillance activities last spring, it also warned that "Communist countries" could be eavesdropping on Americans. The report left a lot unsaid, but it touched off new speculation that the U.S. Government might be up to the same sort of tricks. In an interview last month, Idaho's Frank Church, chairman of the Senate committee also is investigating the CIA, issued an oblique but impassioned warning that the technology of eavesdropping had become so highly developed that Americans might soon be left with "no place to hide." That day may have arrived. *Newsweek* has learned that the country's most secret intelligence operation, the National Security Agency, already possesses the computerized equipment to monitor nearly all overseas telephone calls and most domestic and international printed messages—and that the NSA has made heavy use of its Orwellian technology.

The agency's devices monitor thousands of telephone circuits, cable lines and the microwave transmissions that carry an increasing share of both spoken and written communications. Computers are programed to watch for "trigger" words or phrases indicating that a message might interest intelligence analysts. When the triggers is pulled, entire messages are tape-recorded or printed out. NSA is essentially a military organization, and Defense Department officials deny that civilians are monitored on any vast scale. But *Newsweek's* intelligence sources insist that the agency regularly scans most if not all overseas cables and telephone traffic and a large volume of written domestic communications. Some of the intercepted messages, moreover, have dealt with such civilian concerns as antiwar activism and, reportedly, grain sales to Russia.

Intelligence committees in both the Senate and the House of Representatives have begun to learn about these activities only recently, and the eavesdropping issue will be a potentially explosive feature of their hearings this fall. There are indications that the NSA has begun to cut back on the monitoring program, perhaps because of the attention it has attracted. It is by no means clear, however, that the agency has done anything illegal, if only because technology has far outrun the law; eavesdropping can now be accomplished in ways not anticipated by even the latest anti-wiretapping legislation. Most activities of the monitoring program, moreover, have had a legitimate national-security motive—as well as the impetus that comes from knowing that the Russians do it too—in the U.S.

Secretive: The NSA is so secretive that it almost makes the CIA look like an open book. Even its "charter"—National Security Council Intelligence Directive No. 6—is classified as supersecret. So are most of its other vital statistics, but informed estimates place the agency's annual budget at roughly $1.2 billion (nearly twice the CIA's) and its domestic staff at 20,000 people, plus thousands of military personnel at 2,000 monitoring stations around the world. Headquartered at Fort Meade, Md., the agency has always been led by a military man, and last month, for the first time in the NSA's 23-year history, its director, Air Force Lt. Gen. Lew Allen Jr., 49, testified in public before a Congressional committee.

Allen was not very informative. When Rep. Otis Pike of New York asked for a simple "yes" or "no" to the question of whether the agency was intercepting overseas telephone calls placed by Americans, Allen said the law forbade an answer. The general did expand, however, on the NSA's two missions: "One is that of protecting U.S. communications from foreign intelligence exploitation—this is our communications security (COMSEC) mission. Our other mission is to exploit foreign communications in order to provide information to our own government—this is called our signals intelligence (SIGINT) mission."

Intercept: In simple language, the agency's job boils down to intercepting messages and breaking codes. To do that, the NSA's engineers have revolutionized the art of eavesdropping, and their job has been made easier by the fact that almost all long-distance transmissions of telephone and teletype messages in the U.S. are now carried by microwave, a high-frequency radio signal that bounces between towers spaced up to 50 miles apart. Microwave transmissions are far easier to intercept than messages carried on conventional land-lines—a fact that is only slowly dawning on government officials who regularly send and receive secret information.

The NSA's listening devices—and similar ones developed by the Soviets—can tune in on electronic pulses from microwave transmissions or, less readily, land-lines. The messages are scanned constantly. An interception occurs only when the computers detect a "trigger" word or phrase indicating that the message might be of interest to intelligence or law-enforcement officials—"agent," for example, or "heroin." Instantly, the entire message is recorded or printed out; depending on its content and importance, it may end up in the Pentagon or the White House.

The prime targets of the monitoring are Soviet-bloc diplomats, military officers and espionage agents in the U.S. But almost any communication may be of value to Washington's intelligence analysts. The NSA apparently is interested in data transmitted by multinational corporations, especially oil companies and arms suppliers. Intelligence sources also assume that the NSA monitors news organizations overseas at least occasionally; one reason is that when covering sensitive stories or fast-breaking events, they may have more up-to-date information than government agencies. "Never send the name of a secret source over the air," cautions one official. "They'll get it."

Often, intercepted messages deal only indirectly, if at all, with national security. It is clear from the Rockefeller commission report that for a time the NSA monitored all telephone calls between the U.S. and Latin America as part of President Nixon's war on narcotics smuggling. One of NEWSWEEK's intelligence sources believes that the NSA has monitored all communications traffic having to do with the sales of grain to the Soviet Union. The agency also played a role in Operation Chaos, the surveillance of antiwar activists between 1967 and 1974. Government officials have identified the NSA as the source of 1,100 pages of material given to the CIA on antiwar activities and foreign-travel plans by U.S. dissidents. Indeed, some defenders of the NSA complain that it is too often burdened with work that has nothing to do with catching Russian spies or cracking codes.

One of the thorniest questions facing the NSA is where to draw the line on its communications monitoring. "If you can afford to have this capability—and so far this country has been able to afford it—then there is no sector of signal communications that you can avoid, because any of them could mask illegal activity," says a counterintelligence veteran who has used the NSA's output. If any sort of communication was declared off-limits, this reasoning goes, enemy agents would begin trying to transmit their messages on that particular channel. Carried to its logical extreme, however, that is a license to eavesdrop on everyone.

So far, Federal law does not specifically prohibit the NSA's brand of surveillance. Direct tampering with "wire, cable or the like connection" is illegal. But no one at the NSA has to shinny up a telephone pole and clamp alligator clips onto a terminal box. Instead, the agency plucks electronic pulses out of thin air, and current laws make no mention of the "carrier frequencies" employed by microwave. Thus, the monitoring done by the NSA appears to be perfectly legal, although some courts are beginning to examine that interpretation in cases challenging current wiretap laws.

"Scrambler": In any case, NSA's domestic monitoring activities are paralleled by the eavesdropping of the Soviet Union. To tap electronic transmissions in the U.S., the Russians have set up at least five listening posts across the country, including one at their embassy in Washington and others at Soviet offices in New York and San Francisco. Rooftop antennas enable them to intercept messages carried by microwave—including, apparently, long-distance telephone calls by

U.S. officials. Secure "scrambler" telephones are available, but according to one intelligence expert, "about 90 per cent of the business of government in Washington is done on open phones." According to this source, many government officials do not yet fully appreciate the danger.

The Soviets also have upgraded their spying on military installations in the U.S. Their agents have reportedly managed to bury automated electronic snoopers on mountaintops and desert flatlands near key bases, including the Strategic Air Command headquarters in Omaha, Neb. (Russian diplomats can't travel to sensitive areas, but their surrogates, including diplomats from Soviet-bloc countries, can and do.) The buried units are designed to pop up an antenna from underground to record U.S. military transmissions. When an orbiting Soviet satellite passes overhead, the robot antenna pops up again and transmits the data it has collected.

That kind of eavesdropping may sound like science fiction, but it is mere nuts and bolts compared with breakthroughs that lie ahead in the field of snoopery. Already it is technically feasible to "bug" an electric typewriter by picking up its feeble electronic emissions from a remote location and then translating them into words. And some scientists believe that it may be possible in the future for remote electronic equipment to intercept and "read" human brain waves.

The present and future state of the eavesdropping art gets civil libertarians into a cold sweat. On NBC's "Meet the Press" last month, Frank Church warned that bugging technology "at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything—telephone conversations, telegrams it doesn't matter . . . I know the capacity that is there to make tyranny total in America."

Coups: The NSA intends nothing like tyranny—it is probably the most apolitical agency in Washington. "These people are about as selfless as any group I've every known," says one sympathetic official, and all that available evidence supports that view. The agency appears to have been involved to some degree—"dragged in by the scruff of the neck," one high-ranking intelligence source puts it—into Richard Nixon's short-lived "Huston Plan" for domestic surveillance. Some of the illegal break-ins envisaged under that plan, according to the then White House aide, Tom Charles Huston, who devised it, were necessary to obtain foreign cryptographic material for the NSA. Huston later told a House committee that the NSA had pushed hard for approval of those parts of the plan covering intelligence-gathering breakins, which in the past had led to some major code-cracking coups.

But the central issue raised by NSA's huge eavesdropping network is not really whether the agency has overstepped its authority. The point is that the scientific capability for this wholesale monitoring now exists, and where the capability exists, so too does the potential for abuse. It is the old story of technology rushing forward with some new wonder, before the men who supposedly control the machines have figured out how to prevent the machines from controlling them.

—*Russell Watson with Evert Clark and Anthony Marro in Washington*

[From the Atlanta Journal and Constitution, Sept. 14, 1975]

Military Snooping

PENTAGON LISTENED IN ON AMERICANS' CALLS

(By Charles Osolin)

Washington.—A top secret listening post in Virginia was used by the Pentagon for three years during the Nixon administration to illegally monitor overseas telephone conversations of an unknown number of Americans, it has been learned.

The operation was launched under prodding from Nixon's White House as part of a major effort to stem the smuggling of drugs into the United States, primarily through South Florida.

The listening post—thought to be still in existence—apparently is part of a highly sophisticated nationwide monitoring network costing tens of millions of dollars and maintained by the Pentagon's National Security Agency (NSA) to protect military communications.

Some telecommunications experts say the network also has the capacity for listening in on most long distance calls, telegrams and computer systems throughout the entire United States.

The NSA and the Defense Department declined to comment on the existence of such a system or its reportedly illegal uses. They also declined to say what, if any, safeguards now exist to prevent misuse of the system's Orwellian capability for prying into the personal affairs and business dealings of thousands of Americans.

"I just wouldn't comment at all," said Pentagon spokesman Joe Laitin. "A congressional committee is looking into this and, aside from that, these are intelligence matters. We just don't comment on intelligence matters."

Norman Boardman, information officer for the NSA, said he is under orders to continue the agency's policy of not commenting on any of its activities, capabilities or personnel.

The operation was cryptically referred to in the Rockefeller Commission report on the CIA issued last June. But the Cox Newspapers have learned it was far more extensive than the report implied.

The report said the CIA had eavesdropped on calls between the United States and certain numbers in Latin America at the request of the NSA. It said the operation was terminated after about six months because the CIA's general counsel ruled that it violated federal wiretapping laws.

But there was no hint in the report that NSA had itself done such monitoring for two and a half years before asking the CIA to take it over.

The House Intelligence Committee has since received still-secret testimony to that effect.

One source said the reason the CIA and its professional agents were brought into the operation was because the NSA was concerned that enlisted military personnel working on the project might try to profit from the sensitive information on drug trafficking they obtained.

According to sources familiar with the project, it began in 1970 and involved the NSA, the CIA and the U.S. Navy in collaboration with federal drug agents. It apparently got results.

The sources said the eavesdropping led directly to the seizure of at least one major shipment of heroin worth more than $1 million in late 1972. It may have also played a key role in a series of drug busts in 1971 and 1972 in South Florida during which agents seized more than 800 pounds of heroin worth more than $250 million. These arrests helped dry up the pipeline which then extended from Marseilles, France, through Latin America and Florida to New York City.

But despite its use as a law enforcement tool, the project may have violated the charters of both the NSA and the CIA in addition to the wiretapping violations.

Documents relating to the project have been turned over to the Justice Department, which is examining them for evidence of criminal violations. The Senate Intelligence Committee also will probe the potential threat to privacy.

Committee Chairman Frank Church, D-Idaho, said in an interview the committee first intends to determine what capability the super-secret NSA has for listening in on domestic telephone calls.

"We also intend to find out whether they are now engaged in intercepting such messages and explore the legality or lack of legality for the interceptions," he said.

Church declined to discuss details of the monitoring system or the Latin American narcotics project, saying the committee has not yet "faced up" to the question of how much information can be made public.

He is believed to have had the Pentagon network in mind, however, when he warned in a recent television interview that U.S. eavesdropping technology is so advanced it could enable a dictator to impose "total tyranny" on the American people.

"That capability at any time could be turned around on the American people and no American would have any privacy left," Church said. "There would be no place to hide."

The domestic monitoring system apparently consists of several dozen listening posts manned by Army, Navy and Air Force personnel throughout the United States.

These, in turn, are part of a worldwide system of monitors at more than 150 locations plus an unknown number of spy ships and satellites operated by the military under the direction of the NSA. The agency is headquartered in a heavily guarded compound at Ft. Meade, Md., about 10 miles north of Washington, and draws its personnel from all branches of the military service.

The charter and budget of the NSA are top secret, but it spends the largest portion of the billions of dollars appropriated annually for intelligence activities.

The only station known to have been involved in illegal domestic spying—the one the Rockefeller Commission referred to—is believed to be located at Northwest, a tiny village in the southeast corner of Virginia.

It covers about 4,500 acres on the Virginia-North Carolina border about midway between the Atlantic Ocean and the Great Dismal Swamp and bristles with more than $10 million worth of antennas, radio receivers and computers.

Until the CIA took over the domestic monitoring operation in the fall of 1972, Navy personnel working for the NSA had done the job for more than two years.

One informed source said the system included monitoring thousands of telephone conversations transmitted by microwave and selecting out by computer calls made to and from specific telephone numbers in Latin America.

Tapes of these conversations were sent to NSA headquarters, where pertinent ones were transcribed and turned over to agents of the U.S. Customs Service or the Bureau of Narcotics and Dangerous Drugs.

The law creating the CIA specifically prohibits the agency from engaging in domestic law enforcement or internal security activities.

CIA Director William Colby conceded when the Rockefeller report was issued that his agency's participation in the operation was "wrong—something we shouldn't have done."

But the military, whose role was not then disclosed, has said nothing publicly.

The Nixon White House apparently put enormous pressure on the Pentagon to perform the monitoring service despite its questionable legality.

"A lot of people (in the Pentagon) were troubled about it but there was so much pressure from Nixon that they came down on the side of deciding it was okay," said one source.

Although military personnel assigned to NSA functions are carefully screened, a source familiar with the narcotics project said it was finally decided to turn the monitoring over to the CIA because of the "extreme sensitivity" of the operation.

The source was unable to say if there were actual abuses by the men. But the switch came about a month after revelations of alleged corruption among NSA personnel in the August 1972 issue of Ramparts Magazine.

The magazine quoted Winslow Peck, a former Airman who worked for the NSA in Turkey and Vietnam, as saying "quite a few people in NSA are into illegal activities of one kind or another. It's taken to be one of the fringe benefits of the job—you know, enhancing your pocketbook."

The primary function of the Virginia station is to transmit signals from ships at sea to Navy headquarters in the Norfolk area. The monitoring was only one of its functions.

Although the charter of NSA is secret, recent testimony before Congress disclosed that its intelligence activities are supposed to be limited to "foreign intelligence operations."

The stations operated within the United States for the NSA by the Army, Navy and Air Force are primarily to monitor military communications and ensure that classified information is not discussed openly and that codes and scrambled telephone conversations are transmitted properly.

A telecommunications expert said only four or five sites, strategically located would be sufficient to monitor 90 per cent of all microwave transmissions in the United States. A spokesman for the American Telephone & Telegraph Co. said 70 per cent of all calls in the United States and about half of the overseas calls are transmitted by microwave and thus would be vulnerable to monitoring.

The exact number of military-operated monitoring stations is not known. But in addition to the Virginia facility a Navy spokesman said the Navy Security Group, smallest of the three services, operates

facilities at Charleston, S.C.; Sonoma, Calif.; Winter Harbor, Maine; Ft. Meade, Md.; Elmendorf AFB, Alaska; and about 15 miles south of Homestead, Fla.

The one in Florida is within five miles of an AT&T radio relay center that sends and receives calls from the U.S. Naval Base at Guantanamo, Cuba and a few countries in Central and South America.

[From the Washington Post, Nov. 18, 1975]

Long-Distance Phone Calls Found Easy To Intercept

(By George C. Wilson)

Long-distance telephone calls have become so easy for blackmailers and others to intercept that they should be coded, a Pentagon executive in charge of communications said yesterday.

Intercepting calls that many telephone companies send from city to city by microwave radio "is a simple and straightforward matter for any underworld organization, blackmailer, terrorist or foreign power," said Thomas C. Reed, Pentagon director of communications systems.

Speaking before the Comstock Club of Sacramento, he called on Congress to provide money for scramblers that could make both civilian and military communications safer from eavesdroppers.

"Modern computer techniques make it possible to sort through" the telephone calls radioed from one city to another "and find target conversations fairly easily," Reed said.

Without specifying the cost, Reed said "a small investment in microwave radio scrambled development could lead to secure telephones in this decade." Apparently he envisions private telephone companies employing the scrambling devices the Pentagon wants to buy.

A spokesman for the Chesapeake and Potomac Telephone Co. here said his firm is among those that rely on microwave radio to transmit some long-distance calls because land lines cannot handle them all.

A spokesman for the American Telephone & Telegraph Co. expressed "grave doubts" that intercepting microwave signals would be an easy job, adding that the telephone company has no evidence that such interception has taken place.

He said as many as 30,000 telephone calls in signals—not voice—travel along a microwave beam at one time. He said it would take huge equipment to sift through the signals and reconstitute the conversations.

Reed said that Congress made "drastic cuts" in the Pentagon budget this year and crimped its plans to buy scramblers to protect military communications in the field.

The North Vietnamese and the Vietcong found eavesdropping on American battlefield voice communications, which were not coded, so helpful that they deployed 4,000 to 5,000 men to do the job in South Vietnam alone, Reed said.

"Your and my inability to conduct a private, long-distance telephone conversation requires action," Reed continued. "Those American casualties from ambushes, minings and attacks on helicopters in Vietnam cry out for action."

[From the Washington Post, Feb. 13, 1976]

Fishing Trip Almost Nets Whopper

(By Jack Anderson and Les Whitten)

A top space official, who went salmon fishing last year with Boeing bigwigs, tried afterward to award his fishing companions a "wasteful" $200,000 contract.

The story is told in confidential memos from National Aeronautics and Space Administration files.

The memos identify the obliging space official as Jack A. Jones, a quality control chief based in Houston. He was taken fishing by corporate executives during a visit to Boeing's Seattle headquarters.

Another space official, Joseph H. Levine, was included on the fishing trip but played no part in seeking the $200,000 contract for his hosts.

The incident was turned into drama when the complainant, James Maxwell, died of a heart attack after he brought the scandal to the attention of NASA investigators. Friends say his diligence in pressing the investigation helped bring on the fatal attack.

Maxwell was upset because his name was listed as the NASA engineer who had requested the $200,000 contract. The money was supposed to be spent for research equipment he thought was unnecessary. According to a confidential report, he saw "absolutely no need for this purchase request" and considered it "wasteful to spend (the) money."

It was Jones, not Maxwell, who sought the $200,000 contract for Boeing, the documents charge. Jones allegedly began pushing for the contract immediately after he returned from the fishing trip.

Maxwell complained that the use of his name "implicates me in a violation of law." He died before NASA completed its investigation, which resulted in cancelling the contract. However, Jones and Levine got off with a mild reprimand.

Footnote: A NASA spokesman confirmed that Jones and Levine were entertained by Boeing and acknowledged that Jones sought a $200,000 contract for Boeing after his return. Norman Wynn, one of Boeing's hosts confirmed that the fishing trip took place, called the affair "insignificant" and hung up on our reporter, Marc Smolonsky. Jones and Levine did not return our calls.

Surveillance Subsidy—When local police or prosecutors need special help to spy on alleged criminals, they turn to Uncle Sam for help. During the past seven years, the Law Enforcement Assistance Administration has responded with unusual generosity.

The agency has distributed $160.8 million to support 1,929 intelligence-related projects around the country. The figures were provided to Rep. Bella S. Abzug (D-N.Y.), whose Government Information Sub-committee is investigating federal snooping.

Approximately $2.5 million was earmarked for the "purchase of electronic surveillance equipment," according to the LEAA report provided to Abzug.

Incredibly, $1.3 million of the bugging equipment went to states that either prohibited wiretaps or had no laws on bugging.

California, for example, outlaws wiretapping except in unique circumstances. Yet, the federal government gave California authorities $98,596 for sophisticated surveillance equipment.

The California Department of Justice acquired, among other things 10 "beeper" systems—which allow police to follow vehicles at a distance, 15 voice-activated tape recorders, 26 miniature microphones and headsets, and five "intelligence kits" at $2,500 apiece.

Other states that prohibited wiretaps at the time they received their LEAA grants—Illinois, Kentucky, Louisiana, Michigan and North Carolina—were supplied with body transmitters, auto tracking devices and other unspecified "technical surveillance equipment."

Even when money is doled out to states where wiretapping is legal, there is little method to LEAA's mad giveaway. Official bugging is legal, for example, in New Jersey. There state authorities spent $206,093 in federal funds to buy eavesdropping equipment to handle 808 authorized wiretaps.

But, the report noted, there was "no correlation between the number of wiretap authorizations and the amount of funds expended for electronic surveillance equipment."

Clearly, LEAA exhibits little control over the local spending and use of the equipment. The report points out that 25 states refused to provide LEAA with an itemized breakdown for the bugging equipment bought with LEAA money.

[From the Washington Star, Feb. 19, 1976]

Soviet Ships Tap Phones

Ottawa.—The Soviet Union's fishing vessels and merchant ships operating off Canadian coasts are engaged in espionage, including monitoring of transatlantic telephone calls, according to the top-ranking Canadian naval officer.

Vice-Adm. Douglas Boyle, head of the Maritime Command based in Halifax, N.S., said in a television interview Tuesday night that Soviet submarines observed by Canadians carry missiles capable of hitting Windsor, Ont., from Atlantic waters, and Calgary, Alberta, from the Pacific side.

The program, on the television network of the government-owned Canadian Broadcasting Corp. showed a photograph of a Soviet submarine in a rendezvous with a trawler off the Canadian east coast.

Boyle said that Canadian military aircraft and naval vessels keep the Soviet craft under surveillance. He added that the Soviet activity has forced the Canadian navy to modify exercises in order to keep from revealing tactical procedures to the Soviet observers.

The Soviet surface units perform what the Canadian navy terms "paramilitary" functions, the admiral stated.

"The paramilitary activity centers on the fishing fleet and merchant shipping and the intelligence gathering which they do," he said, "among the fishing fleet are vessels which do, in fact, gather specific intelligence."

Both the fishing vessels and the merchant ships monitor radio communications and radar transmissions, Boyle said. "Many of the people serving (on the ships) are naval persons," he added.

"We are concerned that the amount of intelligence that they might gather which has military significance therefore puts them in a better posture for whatever they might elect to do," he said.

"When we're participating in exercises, and if they show up close to those exercises, it curtails us in the employment of our tactics because we don't necessarily want to show exactly what we do," he said.

[From the Washington Merry-Go-Round, by Jack Anderson and Les Whitten, Feb. 21, 1976]

Untold Story: Buried in the secret files of the National Security Agency is the story of how the agency's top brass used threats to block the production of a low-cost code machine.

The developer of the device, Victor Poor, became convinced that the NSA might firebomb his factory to stop him. Others claimed that NSA merely threatened to take injunctive action in court.

Poor was vice president of a small Frederick, Md., electronics firm in the 1960s. He developed a cheap, teletype-like code machine, which the firm hoped to sell to banks and businesses operating in international commerce.

The machine, costing less than $5,000 apiece, would have permitted these firms to send confidential messages in a nearly unbreakable code.

In those days, NSA was monitoring transoceanic messages in violation of the law. The NSA brass got wind of Poor's device, which they feared would disrupt their eavesdropping.

So out of the blue, the small Frederick firm received a warning call from NSA. This failed to deter the production plans, so the firm's president, John Houston, and attorney, Marx Leva, were summoned to a meeting at NSA's headquarters in Ft. Meade, Md.

Poor has stated on a tape recording that he was told the NSA brass threatened "extra-legal" action if the firm went ahead with the production.

"We don't want you to build it," the NSA officials allegedly warned. "If you do, you're going to get in a pile of trouble."

Poor understood the warning to mean that the factory might be destroyed by arson unless the development of the code machine was stopped. "We'd come in some morning, and the plant wouldn't be there," Poor said on the tape recording.

But Houston and Leva said they don't recall any talk of extra-legal actions. Houston acknowledged that NSA energetically tried to block the production of the code machine but made no improper threats.

"At the time," he explained the NSA's arguments, "the technology was way ahead of foreign countries. If foreign countries had started using it, it would have increased the difficulty of monitoring foreign traffic."

The final decision was not to produce the machine. As it turned out, computerized coding devices far more sophisticated than Poor's inventions were developed not long afterward.

[From Jack Anderson's Washington Merry-Go-Round, Wednesday, May 10, 1972]

THE STRANGE SECRET OF "OPERATION PANDORA"; RUSSIA POURED MICROWAVES INTO OUR EMBASSY; TRIED TO BRAINWASH U.S. DIPLOMATS THAT WAY

(By Jack Anderson)

1972 Pulitzer Prize Winner for National Reporting

WASHINGTON.—Hidden in the Central Intelligence Agency's (CIA) most secret files is an account of a possible Soviet attempt to "brainwash" our embassy personnel in Moscow with mysterious microwaves.

The fantastic details are contained in a file marked "Operation Pandora," which describes how the Russians bombarded our embassy with eerier, low-radiation impulses. Their secret intent, it was suspected, may have been to alter the personalities of our diplomats.

The bizarre story began in 1945 when a Russian presented Averill Harriman, then our ambassador, with a handsome carved Great Seal of the United States. Harriman proudly hung it in the embassy.

The seal contained a tiny electronic eavesdropping device, which monitored conversations inside the embassy until 1952, when it was detected. From this shocking discovery came urgent orders that all embassies must be periodically checked for electronic signals.

In the '60s, U.S. security men discovered the strange microwave impulses, some steady, some pulsating, directed into our Moscow embassy from a neighboring building.

The CIA quickly learned that Russian medical literature suggested microwaves can cause nervous tension, irritability, even disorders. They speculated that the Russians were trying to drive American diplomats stir crazy with the waves.

Neither the CIA nor the State Department had the facilities to test the effects of the silent rays on human beings. At the Pentagon, however, the super-secret Advanced Research Project Agency had worked on electronic sensors and other weird projects.

The agency quietly began a study, under the direction of Richard Cesaro, into the effects of microwaves on people. Cesaro gave the project the code name, "Operation Pandora," and called in a physician, Dr. Herb Pollack, and two crack military scientists, Dr. Joseph Sharp of Walter Reed Army hospital, and engineer-microwave expert Mark Grove of the Air Force.

Sharp and Grove, supplied with the microwave data monitored in the embassy, duplicated the embassy environment, using monkeys for diplomats.

MONKEY BRAIN WAVES

The monkeys actually were trained to perform tasks and then were rewarded with food, much as embassy employees might be rewarded with a dry martini at the end of the day.

The monkeys were studied night and day for months at Walter Reed, while a collateral experiment was also conducted on rabbits by consultant Dr. Milton Zaret in his own laboratory.

In the embassy in Moscow, meanwhile, no one except the highest diplomats and security men were aware of the secret microwave drama.

By 1967, the scientists felt they had watched the monkeys long enough for a tentative reading. Some felt there were signs of "aberrant behavior" caused by the microwaves, but the majority disagreed. Only the rabbits showed clear changes—in their heart rate—which Zaret attributed to heat from the rays.

The disagreement on psychological changes were sent to a top secret reviewing board, which also could reach no absolute conclusion that the rays affected the monkeys' minds.

Nevertheless, the suspicion lingered, and the White House decided that even if the microwaves were not "brainwashing" embassy people, they should be halted. It was also suspected that the waves might be part of some radical new surveillance technique.

At the June 1967 Glassboro meeting between President Lyndon Johnson and Soviet Premier Aleksei Kosygin, the question of the microwave rays came up. One informant insists Johnson personally asked Kosygin to end the ray bombardment, although other sources say the request was made at a lower level.

By 1968, most of Cesaro's scientists were convinced that the microwaves were not psychologically harmful and the embassy experiments ended in early 1969.

The brilliant work done by the team, however, has now led to important research on the effects of microwaves. So far, tests show high radiation can injure eyes, genital organs and perhaps other parts of the body. But, as yet, there is no conclusive proof that low-level radiation is harmful.

Footnote: We have spoken with Cesaro, Pollack, Sharp, Zaret and Grove. All acknowledge they worked on "Operation Pandora," but all refuse to go into details. As Sharp put it: "Pandora was classified in those days and still is."

[From the Washington Post, Mar. 11, 1976]

Two Customs Officers Charged in Bugging

Two federal Customs officers were indicted yesterday on charges of conspiracy and illegally attempting to eavesdrop electronically on a private home in El Paso, Tex.

The Justice Department said the indictment marks the first time that federal law enforcement officers have been formally charged with attempting an illegal bug, during a drug-smuggling investigation.

The two-count indictment was returned in U.S. District Court in El Paso against Michael A. Kelly, 28, of South Hempstead, N.Y., and Henry B. Wade, 26, of El Paso.

Both were Customs Patrol officers stationed in El Paso at the time of the alleged offense, between December, 1974, and January, 1975.

Kelly has since resigned from the Customs Service. Another El Paso man, Terry L. Kirkendall, 29, also was indicted on both counts.

A former Customs Patrol officer, George E. Hough, was named an unindicted to co-conspirator. Hough has pleaded guilty to a federal narcotics charge and is awaiting sentencing, the department said.

The indictment said the defendants conspired to eavesdrop on conversations at an undisclosed residence by using an electronic sensor that had been modified to act as a radio transmitter.

Federal law authorizes federal law enforcement agencies to use wiretaps and bugs only after the Attorney General has approved and a federal court has issued a warrant. That law applies to most domestic criminal investigations.

[From the Washington Star, Mar. 19, 1976]

Telephone Device Pinpoints Those Personal Calls

Boston (UPI).—Those freebe calls you've been making on the company telephone to Aunt Alice in Chicago and Uncle Bill in Miami could prove an embarrassment one of these days.

A Natick, Mass., firm has on the market a system which gives a daily readout of who made what call, when and how much it cost the company.

The printout is available the day after the calls are made, so the boss can immediately confront employes making personal calls on company phones.

That's not its only use, however. Connie Schein, spokeswoman for L. M. Ericsson Telecomm, Inc., said the real savings are realized after the system has been in use for several months, since Telecomm can analyze the phone calls made by a company and recommend less expensive ways to handle them.

Called automatic Identification of Outward Dialing, the system can cut costs 15 to 30 percent for firms with $5,000 a month or more in toll calls, according to Telecomm.

Developed by Bitek International Corp., of Long Beach, Calif., the system is being offered for the first time on the East Coast through Telecomm, a wholly-owned subsidiary of L. M. Ericsson, the Swedish-based international communications system, and New England's largest private telephone company.

AIOD can be adapted easily to any present phone system, according to Telecomm.

Each time an extension is picked up and a call placed, an in-house minicomputer automatically registers which phone is making the call, the day, date, destination and time the call began, time the call ended and the cost. At midnight, a printout of all the information is obtained from the computer.

Although it doesn't monitor the content of the calls, "People who know it's there won't talk as much. It's an automatic control factor," said Miss Schein. "Most business calls can be made within five minutes."

"All operations costs are rising so fast that companies must get full value for every one of their business expenses," said Joel H. Berman,

president of Telecomm. "Telephone use long has been an almost uncontrollable variable in the cost structure, but this system will help bring it under control."

The immediate printout, according to Miss Schein, contrasts with a month or more required by other systems now used on a limited basis in Europe and on the West Coast. Cost is about one-third—a starting price of $30,000 for AIOD, contrasted with a $100,000 range for the others, she said.

The savings are attributed to the fact that AIOD's computer can be directly attached to any printing device, reducing the amount of software between the computer and the printout.

"The equipment will assist the client user in more effective ways to use WATS lines and foreign exchange trunks," said Ernest Lander, Telecomm marketing director and communications consultant. It will enable a user to determine during which days and hours of the day it is best to make expensive telephone calls. "This is called a proper network design," Lander said.

He said the system would be valuable also to businesses, such as law, accounting and engineering firms, which charge their clients for telephone calls. Posting exact charges weekly, rather than having to wait several months, Lander said, would improve cash flow.

[From the Washington Star, Mar. 19, 1976]

Bedroom Bugged, They're Suing for a Million Dollars

'The subsequent hearing of plaintiffs' conversations invaded the privacy and sanctity of plaintiffs' bedroom and intruded plaintiffs' solitude and seclusion.'

—a detail in civil suit

(By Lurma Rackley)

The young man and his wife were dressing to go out to dinner when a loose panel on the lower side wall of the bedroom closet caught the husband's eye. They had lived in the apartment for nearly a year and had never before noticed the panel ajar, so he examined it and made a shocking discovery—a microphone was hanging on a lead wire behind the panel.

Most of the above details are contained in a civil suit filed with the U.S. District Court here Wednesday on behalf of Douglas W. Andrews and his wife, Jacquelin, seeking more than a million dollars in damages and charging the apartment building's resident manager and her husband with invasion of privacy.

Named as defendants in the suit are Katherine A. Kladder, her husband, James, and Dreyfuss Brothers, Inc., the management company for the Hamlet East Apartments where the Andrews lived from January 1974 until shortly after the microphone was discovered on June 11, 1975.

According to the suit, Andrews called Alexandria police shortly after he discovered the microphone about 6:15 that evening. An officer arrived, inspected the microphone, then tugged it free. Trailing behind the mike was a cord about 8 feet long, the suit reports.

Then, according to the suit, the officer went to the apartment directly above the one rented by the Andrews couple to speak with the resident manager.

There, James Kladder showed the officer a closet where the connecting cord hung inside an access panel to the plumbing and also showed the officer a tape recorder which could be connected to the microphone.

Kladder said yesterday he and his wife would have no comment and referred all questions to his lawyer. The lawyer, George Douglas, said, "I have no comment other than we think the case will be dismissed early because we're going to vigorously resist this thing."

Douglas added that the suit is misleading because it implies that the microphone was installed while the Andrews lived in the apartment. "It was done so long ago . . . I don't want to comment any more," Douglas said.

James M. McHale, lawyer for the Andrews, said his clients have moved to Michigan, where Andrews is attached to the Sawyer Air Force Base. He said the entire incident has been a source of embarrassment to the couple. He described them as "very straight" and said they are relieved to be out of the Washington area.

The suit contends that the installation and concealment of the "eaves-dropping device" in the bedroom and "the subsequent hearing of plaintiffs' (the Andrews') conversations, invaded the privacy and sanctity of plaintiffs' bedroom and intruded plaintiffs' solitude and seclusion."

John Fox, lawyer for Dreyfuss Brothers, said the management company was surprised by the incident and does not consider itself responsible in any way.

[From the New Times Magazine, Mar. 19, 1976]

Spies For Hire

While recent criticism directed against the FBI and the CIA may succeed in putting a damper on their covert spying activities, private enterprise remains free to teach similar techniques to interested law enforcement agencies. In fact, spy schools that feature the latest in undercover investigation and industrial espionage have begun sprouting up like weeds. Many are fly-by-night operations, but one of the most successful is Ancapa Sciences of California, an organization that contracts to teach everything you ever wanted to know about computer and electronic surveillance, systems analysis and human factors psychology.

Among its 20 employees are professionals with military intelligence, Law Enforcement Assistance and Drug Enforcement Administration backgrounds. Since its incorporation in 1969, Ancapa has completed contracts with state law enforcement departments in Michigan, California, Texas and Washington, as well as the Drug Enforcement Administration and the Royal Canadian Mounted Police. The company's specialty is the use of criminal dossiers and other information to effectively prosecute suspected terrorists and other radicals.

Ancapa has become a subject of concern to the American Civil Liberties Union in California, as well as to at least one legislator. Perry

Bullard, a state senator in Michigan, is investigating possible civil liberties violations in Ancapa's contract to help the Michigan State Police put several law enforcement divisions under one omnibus anti-radical strike force.

[From the New York Times, Mar. 22, 1976]

Gimbels To Stop Dressing Room Surveillance

(By Frances Cerra)

The New York division of Gimbel Brothers has agreed to stop trying to catch shoplifters by having security guards watch customers as they try on clothes in dressing rooms, Attorney General Louis J. Lefkowitz announced yesterday.

According to the assurance of discontinuance signed by the department-store chain, the practice of watching customers through grilles in the ceiling or high up on the side walls of the fitting rooms has been going on since 1972.

Stephen Mindell, an assistant attorney general said the Attorney General's office had learned about the practice from a December 1975 court decision in which a Manhattan Criminal Court judge had thrown out charges of shoplifting against a Gimbels customer. A female security guard had observed the woman customer in one of the fitting rooms allegedly stealing a scarf. The court found that the practice violated "reasonable expectations of privacy" and the Fourth Amendment to the Constitution.

In signing the assurance, Gimbels admitted no violation of law. According to Mr. Mindell, the position of the Attorney General is that watching customers in the dressing rooms with their knowledge constitutes a "deceptive trade practice."

Gimbels operates seven stores in New York State. Mr. Mindell said he believed that guards had watched customers in most of the stores, but that there might be exceptions.

The store's management said:

"Gimbels security management have evaluated their security procedures used to deter shoplifting and theft and have determined that the surveillance of fitting rooms for apprehension of shoplifters is not necessary. Alternate security procedures have and will be employed by Gimbels to combat this very serious problem."

Asked whether the practice was carried on in all stores, Gimbels management said "No." They said they did not know if this was a common practice in the trade.

Mr. Mindell said that the Attorney General's office was investigating other department stores in New York to determine whether they also spied on customers in dressing rooms. Asked if he had had reason to believe such spying does occur, he said, "Yes, definitely."

[From the New York Times, March 23, 1976]

Inquiry on F.B.I.'s Buying Expanded to All Purchases

(By John M. Crewdson)

Washington, March 22.—The Justice Department's investigation of possible kickbacks to senior F.B.I. officials has been expanded to include scrutiny of all F.B.I. procurements in the last five years, a well-placed Justice Department official acknowledged today.

In light of allegations brought to the department's attention of improprieties in the bureau's purchases of electronic eavesdropping equipment, the official said, the inquiry "necessarily" has been extended to F.B.I. purchasing practices for other items, such as firearms and automobiles.

But lawyers in the department's criminal division, working under John Dowd, a leader of the Justice Department's organized-crime strike force who was handpicked to oversee the sensitive investigation, have not yet developed any firm evidence of kickbacks from any bureau suppliers to past or present senior Federal Bureau of Investigation executives, the official said.

REASON EXPLAINED

Although the official insisted that at this point the Justice Department was "investigating facts, not people," he conceded that the investigation had focused principally on John P. Mohr, the former F.B.I. administrative chief who until his retirement in 1971 was in charge of bureau purchasing.

Mr. Mohr is one of a number of present and former F.B.I. executives who in the last year have attended weekend poker parties in a Virginia hunting lodge arranged by Joseph X. Tait, the president of the U.S. Recording Company, a private concern that buys electronics equipment from manufacturers and sells it to the F.B.I.

The ostensible purpose of that arrangement was to prevent electronics manufacturers from being aware that their products were being used by the F.B.I., and thus being in a position to advise criminals or foreign intelligence agents of the sort of wiretapping, and bugging devices employed against them.

But one such manufacturer, Martin L. Kaiser, who heads a Maryland company, told the House Intelligence Committee last year that U.S. Recording had marked up by 30 percent the prices of some items that it purchased from him before passing them on to the bureau.

LACK IS CITED

Under orders from Attorney General Edward H. Levi, the F.B.I. began an investigation of the relationship between itself and the U.S. Recording Company, but last month Mr. Levi rejected a report of that investigation as unacceptably ambiguous and ordered the F.B.I. to begin another.

One Justice Department official who has read the F.B.I.'s initial report described it today as "wanting." Asked whether it had exonerated Mr. Mohr and other F.B.I. executives who knew Mr. Tait, the official replied that, because of the report's ambiguity, it was "hard to say."

[From the Times (London, England), Apr. 9, 1976]

'Skyspy' Can Put Enemy Activities on Television

(By Arthur Reed)

The security covers were removed yesterday from a British robot "spy in the sky" which can fly over enemy territory sending back television pictures to its base miles behind the lines.

Called Skyspy, it has been developed by the Belfast-based aircraft manufacturers, Short Brothers and Harland, as a private venture, and has logged 70 hours of tethered flight. Short Brothers will now ask the Government for financial support to develop the robot further for the British forces and as an export venture for sale to foreign forces.

Two Skyspys would be able to carry out continuous surveillance of the border between Northern Ireland and the Irish Republic.

Skyspy has the appearance of a large ventilation fan, with its propeller enclosed in a circular casing and its cameras slung underneath. It takes off and lands vertically.

Short Brothers said yesterday that the small size of the robot made it difficult to detect. Possible uses included army reconnaissance, naval viewing over the horizon, target spotting, weapon control and delivery, coastguard surveillance, border patrol, fishery protection, traffic control, search and rescue operations and forestry observation.

It could also be used for electronic countermeasures and, with an airborne laser mounted, for helping to guide missiles. In addition it could attack armoured vehicles on the ground, delivering a warhead with high accuracy and immediately relaying the results to its base without hazarding skilled men or expensive equipment.

A considerable programme of precision hovering had been carried out so far, Short Brothers added. The safety restraints would be gradually eliminated so that the vehicle could begin a further development programme of unrestrained flight trials.

[From the New York Times, Apr. 11, 1976]

Rights Unit Seeks End to Lie Tests

EXAMINATIONS CALLED UNFAIR TO POTENTIAL EMPLOYEES

(By Peter Kihss)

One of every four potential employees tested by companies may be barred from a job because of recommendations by polygraph operators, according to the New York Civil Liberties Union.

The group considers such lie-detector tests to be of "unproven reliability" and a threat to individuals' privacy. It is backing a bill passed by the Assembly at its current session that would prohibit employers in New York State from requiring lie-detector tests in connection with jobs.

The bill by Assemblyman G. James Fremming, Democrat of Erie County and a retired Buffalo policeman, would make violation a misdemeanor subject to a fine up to $500. An employee's waiver or voluntary submission would be no defense, according to the bill, now in the Senate Labor Committee.

A memorandum by the civil liberties group, released by its legislative director, Barbara Shack, cites the United States Senate Judiciary Committee as reporting estimates that nationwide 3,000 examiners have been giving 200,000 to 300,000 polygraph tests a year.

REJECTIONS ON THE RISE

Mrs. Shack said in an interview that rejections of job applicants jumped from 2 percent, after traditional background screening and reference checks, to 40 percent, after use of polygraphs, according to a 1966 report by the Illinois Retail Merchants Association.

Thirteen states already prohibit employers' use of lie detector tests in various ways, according to the civil liberties memorandum, they include New Jersey, Connecticut, Pennsylvania, Massachusetts, Delaware and California.

The New York Legislature passed proposed prohibitions in 1967 and 1970, but the bills were vetoed by Gov. Nelson A. Rockefeller.

On the national level, the House Committee on Government Operations recommended last February that "the use of polygraphs and similar devices be discontinued by all government agencies for all purposes."

The Senate Judiciary Committee in 1974 proposed legislation to bar both private industry and Federal agencies from "requiring, requesting or persuading any employees or applicant for employment to take any polygraph test."

Mrs. Shack's memorandum noted that the polygraph, which records breathing, blood pressure and skin reactions simultaneously, is the most commonly used lie detector.

Other techniques include two types based on speech variations—a psychological-stress evaluator and a voice analyzer. A so-called "wiggle seat," the memorandum said, can be rigged into an office chair to measure changes attributed to nervous movement. Other devices are "microwave respiration monitors" "pupil dilation," measures.

The civil liberties memorandum said that "employee complaints of abusive practices have reached an acute level."

Lie detectors were said to be used not only to check on possible thieving but "to acquire personality profiles on employees and to thereby root out deviant behavior, unpopular political beliefs or simply different opinions."

"Once the test begins the privacy of the subject is abandoned," the memorandum said. It asserted that "rarely is there follow-up to confirm the judgment of the operator," and "it is simply easier not to hire the individual."

A 1964 study was cited as estimating that only 20 per cent of the then lie-detector operators were "duly qualified."

The memorandum said that Federal and state courts have held test results inadmissible as evidence. Some persons, such as actors and yogis, it added, can "control their responses to such an extent that they are able to 'beat the machine,'" while "pathological liars . . . are impossible to discover."

[From the Wall Street Journal, April 15, 1976]

The Future Revised*

Conventional Warfare Changing Faster Than the Experts Predicted

The Vietnam War Hastened "Automated Battlefield," But Costs May Retard It

Ready for the Wrong Fight?

(By Richard J. Levine)

Washington.—Not long after the latest Mideast war, Malcolm Currie, the Pentagon's research and development chief, sketched for Congress his vision of war in the future.

Tactical advances, he said, foreshadowed "a true revolution in conventional warfare." Some of the new technology, in its Model-T stages, has already been proven in combat: unerring, precision-guided bombs and missiles, unmanned aircraft, remote electronic sensors. "Advances such as these, further developed and widely applied," he said, "can change a broad spectrum of conventional warfare in the next decade in the way tanks once revolutionized ground combat and radar revolutionized air defense."

As the Wall Street Journal again explores the nature of war in the year 2000, it's useful to note that military experts 10 years ago failed to foresee the rapid emergence of the "automated battlefield" that already is becoming a reality. Though the technology of automated warfare was understood, the war in Vietnam greatly accelerated actual development.

Missing the Big Changes

Nor was that all the experts missed. They failed to anticipate most diplomatic, political and economic developments that have had a profound influence on military thinking and planning. They had no notion of a U.S.-Soviet agreement to limit offense nuclear weapons, or of détente generally. They had no hint that American involvement in Vietnam would create a strong anti-military mood, ending for at least half a decade of defense budgets. Nor was there any sign that the U.S. would abandon the draft in favor of costly volunteer forces and that manpower expenses would consume 55% of the defense budget.

---

*Ten years ago, the Wall Street Journal began publishing a series of articles dealing with life in the year 2000. Developments in the past decade have changed the outlook. This is the last story in a new series examining some of those developments and their implications.

Finally, the experts were unable to foresee the explosion in the cost of modern weaponry fostered by inflation, the increasing complexity of weaponry and production problems. In 1967, weapons planners usually assumed that if something new and exotic could be built, it would be built. Today, cost constraints threaten to keep many futuristic plans on the drawing boards. Thus Pentagon experts are more cautious in their long-range predictions than their predecessors in the mid-1960's.

The U.S. is unlikely to become a garrison state. By 2000, one Pentagon forecast has it, military budgets probably will take up less of the gross national product than they do today—less than 5% compared with the current 6%. Inflation will eat up much of the increase in dollars, so that many analysts believe U.S. forces will number fewer than today's 2.1 million uniformed men and women.

A simple projection of current cost trends is unthinkable. If they do continue for a few more decades, says Army under secretary Norman Augustine, "we will quite literally be able to afford only one (type of) aircraft or, for that matter, one tank and one ship.

TOP PRIORITY TO NUCLEAR ARMS

"Cost is a huge consideration," says an Army general who oversees research and development. "We just have to consider the affordability of these modern technologies."

Still, much of the military hardware that will be in use at the turn of the century is already visible in research and development centers, because it can take 15 years to move a complex new creation from the research stage to active duty.

Twenty-five years hence, defense experts expect that strategic nuclear weapons, designed to deter atomic war, will still enjoy top priority. The arsenal is likely to consist, as it does today, of a mixture of land-based missiles, submarine-launched missiles and long-range bombers. But there will be important new departures.

Today's Minuteman III intercontinental ballistic missile will be supimplemented by the large M–X, a missile that may be more mobile and so less vulnerable. The giant Trident submarine, just going into production, will be the backbone of the undersea strategic force. The B1 bomber, scheduled to move into production late this year, will still be on duty; it could be beefed up with highly accurate cruise missiles—jet-powered computer-guided missiles that fly low and slow to escape radar detection.

UNMANNED FIGHTERS

For conventional ground warfare, the Army will be equipped with a new tank and a new mechanized combat vehicle that, in effect, allows an infantry squad to fight while riding. It will have electronically guided artillery shells that can easily hit moving tanks, a heat-sensitive infrared sensor system that allows soldiers to "see" through darkness and smoke, and "instant minefields" that can be fired by artillery or aircraft on advancing enemy troops.

The Air Force will still man fighter planes. But unmanned aircraft called remotely piloted vehicles (RPVs) will fly many reconnaisance and bombing missions and some might be ready for air-to-air combat. Weapons delivered by the planes and RPVs will be much smarter

than today's "smart" bombs, able to find and destroy their targets at night and in bad weather. Earth-orbiting satellites probably will help guide them.

Naval warfare seems less likely to change. At any rate many U.S. admirals insist that large nuclear-powered aircraft carriers should continue to be built at a cost of nearly $2 billion each. Still, defense experts in and out of government think the day of the giant carrier is nearing an end, and the search for a replacement is on. A Navy study suggests a relatively austere "air-capable" ship of about 10,000 tons that would be armed with antiship and antiaircraft missiles and vertical-takeoff fighter planes.

Even as they plan these and other weapons, however, defense officials have nagging doubts that they are preparing for the right kind of war. Ever since the withdrawal from Vietnam, the military establishment has turned its attention toward a possible land war in Central Europe, where 30 years after World War II, 600,000 European soldiers and 200,000 GIs still face 925,000 Soviet-led troops.

"For the foreseeable future we will continue to shape our forces against the only guys who pose a substantial threat," an assistant defense secretary says. "But the sophisticated weapons we're developing to take on the Soviets aren't the ones I would want for trouble with India or Panama."

Indeed, a growing number of defense analysts believe that the greatest danger to the U.S. in the closing years of the century will come from poorer, less industrial nations, and most likely in the form of terrorism rather than conventional warfare. "Between now and the year 2000, I think there is a major opportunity for a shift from East-West confrontation to North-South confrontation," and Air Force strategist says "We've already seen the first evidence of this—inplane hijackings, kidnapings and mail bombs."

In his study on "Transactional Terror," J. Bowyer Bell, a researcher at Columbia University's Institute of War and Peace Studies, found the U.S. a likely target for foreign terrorism. "Revolutionaries from abroad, attracted by soft targets, may strike at what they see as the center of the imperialist-capitalist-racist conspiracy," he said.

NUCLEAR TERRORISM

Large, complex industrial societies are increasingly vulnerable to the new generation of small, easy-to-operate, highly accurate missiles. Brain Jenkins, an analyst at the Rand Corp. "think tank", says such weapons "will undoubtedly find their way into the hands of terrorists." He asks: "What will happen when the Saturday night special' is not a revolver but perhaps a hand-held, laser-guided missile?"

A special horror is the prospect of terrorists armed with nuclear weapons, raising the spectre of what Mr. Jenkins calls "political extortion and mass-hostage situations on a scale that we have not yet seen." Other researchers worry about outright nuclear warfare touched off by the proliferation of nuclear weapons. Five members of a Harvard University-Massachusetts Institute of Technology study group concluded last year that nuclear war is likely to erupt before 1999, most probably between smaller nations in the Mideast, perhaps, or Africa.

"There are going to be an awful lot of people with nuclear weapons, and it's going to be awfully important to be able to intercept one or two of those weapons," a top Army official says. By a 1972 treaty, the U.S. and the Soviet Union each limited itself to a single antiballistic missile (ABM) site, and the U.S. is now abandoning its site in North Dakota. Now some analysts believe that the U.S. eventually will have to build new ABM defenses against threats from terrorists and smaller powers.

An Air Force general thinks an answer to such threats may lie in high-energy laser weapons, based in space, capable of destroying missiles with thin, powerful light beams. The Pentagon is spending some $200 million a year to develop more-powerful lasers. In this and in other research and development, however, defense officials are encountering serious technical and cost problems.

ARMS RACE TO CONTINUE

Such problems befell certain weapons projects described in this newspaper's 1967 look at war in the future. At the time, for example, the MBT–70 "dream" tank was to go into service in the early 1970s. After nine years of development. Congress killed the MBT–70 program in December 1971. The House appropriations committee saw it as "unnecessarily complex, excessively sophisticated and too expensive." It would have cost $1 million a vehicle and, the committee said, "no tank is worth that much money."

Most experts assume that the U.S. and the Soviet Union won't fight a nuclear war. But the strategic arms race, they think, will continue, only slightly slowed by arms control agreements. The U.S. is making modern its entire arsenal of long-range weapons. It is spending 2.5 billion to research and develop an ICBM more powerful and less vulnerable than the Minuteman III.

Decisions on how and where to base the new M–X missiles will be tricky. Three alternatives are under consideration: Hardened, underground silos like those housing the Minuteman; mobile "transporters-launchers" and large aircraft. The Air Force explored the latter alternative by dropping a Minuteman I from a C5A cargo plane and igniting the missile in mid-air. Completion in 1984 of a new system of 24 NAVSTAR communications-navigation satellites would improve the accuracy of that kind of delivery system.

The shape of the next generation of missile-firing submarines and long-range bombers is clearer. General Dynamics already has contracts for construction of the first three of 10 Trident submarines. The huge, nuclear-powered Tridents, to be launched by the end of this decade, will each carry 24 nuclear missiles with ranges of 4,000 miles at first and 6,000 miles in later versions. The current cost of each submarine with missiles is more than $1.6 billion.

The new bomber will be Rockwell International's B1, barring abandonment of the controversial plane by some future Congress or President. Critics think it is obsolete already and that, at nearly $87 million a plane, it costs too much. But the first test bomber flew in late 1974, and the Air Force is pushing for a production go-ahead late in 1976.

On the ground, the 1973 Arab-Israeli war most convincingly illustrated the potential of the kind of automated combat born in Viet-

nam. Many Western military observers saw in the Mideast war the emerging superiority of new defensive weapons against the tanks and fighter-bombers that had dominated battlefields since World War II.

One of the Army's most striking advances is a laser-guided artillery shell known as the cannon-launched guided projectile. It promises to make tanks even more vulnerable in the future than they are now. They would be targeted by small, unmanned aircraft with television cameras and laser beams. The projectile would home in on the laser-designated target. In tests, the shell has hit a moving M48 tank. In effect, it would turn artillery into sniper weaponry.

NAVY'S NEW-OLD ROLE

The world got its first sustained look at similarly guided airborne projectiles in Vietnam. A designator aircraft would focus a laser beam on a target, and a second plane would drop a "smart" bomb, equipped with a device to sense laser light reflected from the target and adjust the bomb's steering vanes toward it. Such precision-guided weapons today can hit targets 50 miles to 100 miles distant, but not in fog or darkness. In the future, they will operate in any kind of weather. And they may be programmed to choose targets: a tank, say, rather than a mere jeep.

At sea, Navy men think that 25 years hence, one of their prime missions will be the protection of surface shipping for a nation that will be importing even more raw materials, especially oil, and exporting even more agricultural and industrial products.

The high cost of building superfast warships, and technical and other difficulties, have dimmed their lustre. Some Navy men suspect the basic warship of the future may resemble a rather unspectacular design, the ACV–G, or advanced aviation guided missile combatant. Essentially it would be a box 450 feet long, 150 feet wide and four stories high, riding out of the water on two submarinelike structures. Its open decks could launch a dozen vertical-takeoff planes, and it would be armed with antiship, antiaircraft and antisubmarine missiles. Its top speed would be 40 knots, not much faster than today's carriers.

[From the New York Times, Apr. 18, 1976]

Polygraph Tests Barred C.I.A. Jobs

SIXTY PERCENT OF APPLICANTS REJECTED OVER 11 YEARS—REP. ABZUG TO SEEK CURB ON DEVICES

(By Peter Kihss)

The Central Intelligence Agency has disclosed that more than 60 percent of its job applicants rejected on security grounds from 1963 through mid-1974 were turned down on the basis of polygraph, or lie-detector, interviews.

Representative Bella S. Abzug, Democrat of Manhattan, made public yesterday statements that she had received from the C.I.A., the

Defense and Treasury Departments, Federal Reserve Board and Postal Service upholding use of polygraphs for various purposes.

Asserting that "the polygraph cannot distinguish truth from falsehood," Representative Abzug said she had introduced a bill that would make it a criminal offense to administer polygraph tests in connection with jobs in the Federal Government.

She said the bill would also apply to private employers involved in interstate commerce or dealing with the Government.

Mrs. Abzug said the proposed bill would not apply to the use of polygraph tests in criminal investigations.

The statement by George Bush, the new director of Central Intelligence, said that about half of the agency's job applicants rejected because of polygraph test information "had already completed all other security screening and been provisionally approved on this basis."

"Without the polygraph program," Mr. Bush wrote, "the disqualifying information on these cases would have remained unknown. In addition, it is reasonable to presume that the program is a significant deterrent to application for employment by unsuitable candidates, and more importantly, penetration attempts by foreign intelligence services."

Mr. Bush said the agency had "adopted strict procedures to prevent abuses," including notifying each applicant about the use of polygraph tests, medical determination if a polygraph interview is advisable, warning that a privilege against self-incrimination exists, and limiting questions to "security issues."

Mrs. Abzug is chairman of a House subcommittee on Government information and individual rights whose studies led in February to a report by the House Government Operations committee recommending a complete ban on the Federal use of the polygraph and similar lie-detector devices.

Mrs. Abzug said that since the recommendation there had been reports that the C.I.A. had "resumed use of polygraphs for periodic testing of its employees" as a result of unauthorized disclosures from Congressional committees investigating intellegence practices.

Terence E. McClary, Assistant Secretary of Defense, said in a letter to Mrs. Abzug that the Defense Department had moved to upgrade the polygraph program over the last few years and had adopted limitations "to insure the protection of rights of all individuals." He said a new "objective assessment of its utility in the investigative process" was underway.

For the Treasury Department, David R. MacDonald, Assistant Secretary for enforcement operations and tariff affairs, said, "The polygraph is used sparingly by Treasury enforcement agencies as one among many investigative techniques," but "it is not a general exploratory mechanism."

Arthur F. Burns, chairman of the Federal Reserve Board, said polygraph tests were given to employees of four Federal Reserve Banks last year, all in cases involving criminal larceny. Most, he said, were conducted "at the suggestion of or with the concurrence of the Federal Bureau of Investigation."

Mr. Burns said he believed "polygraph devices should not be used to screen applicants or for other personnel inquiries."

Postmaster General Benjamin F. Bailar said the Postal Ingraph tests "in some criminal investigations to narrow a list of suspects after other investigative methods have failed." He said "the greatest benefit" was in clearing innocent employees, and tests were "on a voluntary basis."

Mrs. Abzug said the Justice Department "consistently opposes the admission of polygraph evidence at trials" but sent her "no substantive reply or acknowledgement on her inquiries regarding the device."

Agencies using polygraphs, she said, also include the Customs Service, the Drug Enforcement Administration and the F.B.I.

The New York Representative cited estimates that 200,000 persons undergo polygraph tests each year in preemployment or employment situations. Her bill would make its use in such cases a misdemeanor punishable by a fine of $1,000 and allow Federal Court suits for damages.

[From the Washington Post, May 2, 1976]

Fifty Thousand Subjected to Legal Wiretaps

(By Margaret Gentry)

Federal and state investigators used listening devices and telephone taps to eavesdrop on nearly 50,000 people last year, but what they heard, more often than not, was innocent conversation.

Those conclusions emerged from the government's annual statistical report on court-approved wiretaps and bugs. The report, issued Friday, was prepared by the Administrative Office of U.S. Courts.

Federal and state investigators obtained court warrants for 701 taps and bugs in 1975, actually installing them in 676 cases, the report said. The figures mark a 4-percent decrease from the previous year.

The report said each case of eavesdropping intercepted an average of 654 conversations involving 71 persons. An average of 305 conversations, or about 46 percent, were considered incriminating, the report said.

According to the government statistics, investigators overhead nearly a half-million conversations, but concluded that more than 235,000 of them had nothing to do with criminal activity.

The report showed that five cases of electronic surveillance produced no incriminating evidence at all, although 652 conversations involving 68 persons were overheard.

Two of those cases were under state warrants in New York, and one each under state warrants in New Mexico, Florida and Massachusetts.

The report said federal taps and bugs produced a somewhat higher proportion of incriminating evidence. It said 67 per cent of the conversations heard by federal agents were considered incriminating.

The 1968 federal law authorizing taps and bugs in certain criminal cases requires investigators to "minimize" the interception of innocent conversations.

But law investigators complained they often can't determine that a conversation is going to be innocent until after listening to all of it.

The report showed that federal and state officials shy away from using bugs, the tiny microphones planted in rooms or cars to transmit conversations to tape recorders elsewhere.

Federal authorities used only 11 bugs and 12 combinations of bugs and telephone taps. States used 26 bugs and seven combinations.

The National Wiretap Commission, in a separate report Friday, urged wider use of bugs and phone taps and said judges should specifically authorize investigators to break into private premises to plant bugs.

[From the Washington Post, July 3, 1976]

The Federal Diary

Abzug Lends Ear on Phone Tapping

(By Mike Causey)

Federal workers who think their office telephone calls, business or personal, are being bugged now have a sympathetic ear on Capitol Hill.

Rep. Bella Abzug (D-N.Y.) has become the central exchange for civil servants who believe the popping, clicking or other tell-tale noises on their lines indicate Big Brother or Big Sister is also on the horn.

Some agencies apparently still monitor lines for training purposes or to determine if workers are being helpful and courteous to the public, or to catch suspected bad guys.

Some, apparently, have used the eavesdropping technique to find employees who were abusing federal lines and time to call friends, relatives or even long-distance bookies and business associates about nonfederal business.

Although it is unknown which agencies, if any, are now bugging lines (the preferred term is "monitoring"), workers at the CIA, NSA and in some Defense offices assume that internal security is listening in.

Abzug is interested in who is listening to whom, and why, because she chairs the House Subcommittee on Government Information and Individual Rights. One of those individual rights, many people believe, is the guarantee that even a government worker can use a telephone without persons unknown listening in.

Abzug has been hearing from employees and union leaders who think Uncle Sam ought to be able to draw the line between monitoring to fight crime and the overzealous use of telephone taps by government officials who sometimes become paranoid on the subject of what is being said on the telephone.

[From the Washington Post, July 22, 1976]

The Age of the Electronic Passport

(By Benjamin Welles*)

Weary American tourists, shuffling through the airports of the world while glazed-eyed minions whack rubber stamps into their passports, may take heart. Within five years a "machine-readable" passport will probably be adopted the world over, and then shuffle-time will be, if not eliminated, substantially cut.

The prime impetus stems from the fact that the U.S. Passport Office, a semi-independent and much-neglected fief of the State Department, is in danger of grinding to a halt—victim of soaring demand (2.7 million passports this year alone), obsolete equipment and outmoded facilities.

Its ancient "flexo-writer" passport machines, for instance, date from the late 1950s—and are no longer made. Frances Knight, the soft-spoken but indomitable U.S. passport director, has recently had to hire a $50-a-day mechanic just to keep the 26 machines in her headquarters here from breaking down. At passport offices across the nation (and abroad) employees are still affixing photographs with Elmer's glue and hot irons. In this split-second world of electronics, the whole system is still linked by old paper-tape machines plodding along at 75 words per minute.

For six years Miss Knight and her staff have been seeking State Department and congressional approval for $20 million to replace the old system with cathode ray tube in-put terminals, mini-computers, high-speed computer printers and encoding machines. The planned overhaul, they say, would speed service to the public, help eliminate fraud, cut rising costs and in the first 10 years save an estimated $38 million.

Foreign countries, too, are facing mounting problems as populations grow and more people travel. To bring order out of chaos, a 10-nation committee of the International Civil Aviation Organization (132 members) came up two years ago with recommendations for an internationally standardized, smaller, passport (3.7 by 4.9 inches) easy to slip into pocket or purse and thus less liable to loss or theft. Miss Knight was the U.S. delegate, and so next year's passports will reflect some, if not all, the new recommendations.

ICAO made one proposal, however, that is worrying the State Department, the White House and Congress. It recommended that the personal description of the bearer in the new passport not only be readable to the human eye—but also "machine-readable" through the insertion of a small magnetic strip (like those on the back of many credit cards). The personal details would also be invisibly coded onto the strip. Most countries would go on using inspectors with rubber-stamps; the technologically advanced nations (which get most tourists) would gradually install electronic "readers" at their ports and airports.

It is this machine-readable proviso that is worrying civil libertarians here—and in ICAO, too. One scenario, drawn by technicians,

* Mr. Welles is a former New York Times correspondent.

is chilling. An American traveller lands with the new-type passport at, say, Orly where the new machine-readable system has been installed. He slips the ionized back page of his new U.S. passport (with its magnetic strip) into the electronic reader. Computers in a nearby security-police office spin. There is nothing on him—he is on his way in seconds.

But perhaps he is on some list—Interpol or other—and the computers "flag" him. Within seconds a secret alert can be automatically encoded into the magnetic strip—warning police everywhere in that country, or even in neighboring countries, to place him under surveillance—however innocent his journey. When he departs, the coded alert can be automatically erased and he will never be the wiser. "Big Brother" is at hand.

To guard against invasion of privacy ICAO recommended limiting the total of personal details, visible or invisible, on the proposed passport to 92 characters. No name, it was felt, would require more than 33 characters and the rest would adequately cover other requisite information: date, place of birth, sex, issuing authority and expiration.

"But ICAO also recognized that governments don't necessarily trust each other," observed one informant, "so it stipulated that the 92 characters would have to be "frozen" magnetically before the new passport could be universally adopted. The idea was to prevent accidental erasure—or, worse, clandestine alteration."

The problem is that no fool-proof system of magnetically "freezing" coded information has yet been developed, although such technologically sophisticated firms as 3M and ITEK in the United States and Britain's EMI, all claim to be nearing a breakthrough. In any event, the outcome will depend on cost: Will it be both inexpensive and fool-proof?

ICAO's experts are due to meet here again in September and, if by then some "freezing" technique has been developed, probably the U.S. and the ICAO membership will push for a book-type but machine-readable passport. At earliest it is still about five years away—and even then it will represent a compromise between the great majority of nations still using inspectors with rubber stamps and, for example, the European Common Market nations whose citizens already cross each other's frontiers with machine-readable laminated plastic identity cards.

If no "freezing" techniques are ready by September, ICAO and the United States will probably recommend a passport that can be "optically scanned." This is a slower, more costly system, but it is already in use. The U.S. Immigration and Naturalization Service, for instance, is perfecting an electronic, hand-held "wand," tied to a computer, that can be passed over the laminated plastic identity cards being issued to Mexican and other aliens who cross in and out of the United States frequently. By using "algarithms"—coded combinations of letters and numbers—counterfeit documents are quickly spotted.

Frances Knight has told Congress that she is not "wedded" to the machine-readable passport; that optical scanning or any other viable system will do provided the system is soon overhauled to cope with the rapid rise in world travel. So long as she is in charge, she says, there will be no national identity cards or national registration. Her

prime concern is accurate, rapid screening of applicants for passports—and elimination of fraud.

"Fears about Big Brother and a police state are exactly why the Passport Office needs its own computer with no outside access to anyone," she said in a recent interview.

[From the Washington Post, July 25, 1976]

Big Brother's Sensors

(By Paul Dickson*)

The White House lawn, Disney World, the border between the United States and Mexico, an exclusive subdivision in the Maryland suburbs of Washington and a number of other places and institutions have one thing in common: They are, to varying degrees, making use of the sensors, night-vision devices and other technology of the Southeast Asian war.

Like their military counterparts, civilian users have, for the most part, not been reluctant to come across with success stories. Army Starlight Scopes have been pressed into service by Park Service rangers to apprehend wrong-doers working at night, such as alligator poachers in the Everglades. A heat sensing camera used to detect traffic along the Ho Chi Minh Trail has been pressed into service (along with the Navy patrol plane that carries it) by the Environmental Protection Agency to spot water polluters.

There is a growing collection of stories about night-vision devices in police work, which run the gamut from a Boston situation in which a major narcotics transaction was watched in the dark, leading to a major arrest, to a Linden, N.J., sniper incident in which just prior to the moment the police opened fire on the suspected gunman the night-vision device showed that the man who was about to be shot was another policeman. Los Angeles County firemen now use night-vision goggles as they direct night and low-visibility forest fire fighting operations from helicopters, and, as has been pointed out in a national advertising campaign, an ITT light-amplifying device developed for the Army is now used experimentally to help those suffering from retinitis pigmentosa, a blinding disease that often makes it especially difficult for those afflicted to see in dim light.

Sensors have been put to use selectively in a number of situations in which the goal is to detect interlopers. They have been used experimentally at airports to head off cargo theft, by a Delaware telephone company to protect against pilferage of copper parts, in home security applications such as the Maryland suburb, by Customs and Drug Enforcement Administration officials in keeping tabs on the traffic at remote and deserted airstrips and, according to a report in Electronics magazine, by the Secret Service to keep the seismic pulse of the White House grounds. For every actual installation there are a number of proposed civilian sensor applications for such places as nuclear power plants, warehouses, government installations and the like.

---

*Dickson is the author of the book, "The Electronic Battlefield," published by the Indiana University Press, from which this article is excerpted.

Of all the applications of sensors to date the most ambitious has been the McNamara Line type of fence erected along portions of the border between the United States and Mexico. This all began in 1969 with the Nixon administration's Operation Intercept to cut drug smuggling between the two countries. At the time, Intercept director Eugene T. Rossides pledged the most modern military equipment would be thrown into the effort and this included both airborne sensing devices and unattended ground sensors.

These early uses of ground sensors were effective and within a year John Mitchell's Justice Department was seeding a 65-mile experimental stretch of the border with Vietnam-tested acoustic sensors, buried strain-sensitive cables and infrared detection devices. In 1972, when the test section was fully operational, 128,889 illegal crossers were apprehended and authorities claimed more than 30,000 were netted as a result of the electronic fence. In the fall of 1973 the U.S. Border Patrol and Immigration and Naturalization Service jointly announced plans to expand the fence along the whole 2,000-mile border with the exception of the most inaccessible areas and immediately pledged $1.5 million to start the job.

Today electronic sensors are installed at the most active points along the border, but there is some question at the moment whether the whole border will be wired. This situation results largely from the success of the system (although costs have been a factor too). Gen. Leonard F. Chapman Jr., head of the Immigration and Naturalization Service, explained in a 1975 interview in Nation's Business that the sensors work fine but that more than half the alarms go unanswered because the Border Patrol is spread too thin.

HIGH COSTS

While most of this spinoff of hardware has been benign or downright useful, it does not take that much imagination to envision devices plugged in and wired down at such a rate and for such purposes that we are soon at Orwell's nightmare state in which there is ". . . no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guess work. It was even conceivable that they watched everybody all the time." Within such a context there is a definite chill in such bits of recent news as these:

The FBI has recently purchased two Army planes equipped with the most sophisticated airborne sensing devices. Some have wondered aloud if this could be the first buy in an FBI airborne surveillance force.

Increasingly, companies possessing the technology are advocating sensors and associated items for a bigger and more diverse market which should soon get down to the man on the street. The technology is ready. Several companies have devices able to discriminate between people and pets. Some of the new general market sensors appear to have the capacity to fulfill a Big Brother as well as a crime-stopping role. For instance, a new sensor from GTE Sylvania responds when one touches or even comes very close to a metal object such as a desk or filing cabinet. One sensor can keep track of 20 desks.

The police in a number of communities across the country are now able to keep tabs on whole neighborhoods through the use of 24-hour

closed circuit TV systems. The first operation of this type was installed in a section of Mount Vernon, N.Y., by Sylvania with the help of a $47,000 grant from the Justice Department. "Only time will tell," said a Sylvania paper on its system, "if citizens will object to a 'Big Brother' type atmosphere." A number of systems have followed but in terms of the latest in Buck Rogers urban technology it would seem hard to beat a 2-square-mile area on Cleveland's East Side where low-light-level-color TV images are sped to police headquarters by laser beam.

There can be little question that all of this is proliferating despite its expense. A Star-Tron night vision device for police costs between $3,000 and $5,000 depending on its size, and a knowledgeable expert estimates that the job of sealing the whole Mexican border with sensors will cost hundreds of millions of dollars. To see this proliferation one need only stroll through the hardware display areas of such affairs as the annual International Security Conference or look through the list of current R & D grants from the Justice Department's Law Enforcement Assistance Administration or scan the papers given at the heavily electronics-oriented Carnahan Crime Countermeasures Conference put on each year by the University of Kentucky. At the Carnahan Conference one is likely to glean any number of leads on the future shape of police electronics such as a 1973 paper given by researchers from the Plessey Radar Research Center in Great Britain, which reported progress on a new sensor for detecting cadavers by sensing decomposition. Just the thing for finding bodies. There may be a lead in this for military electronics, too; one wonders if perfection of the body sensor might lead to the automated body count. Significantly, some of the financing of this electronic marvel comes from the U.S. Army.

Even more to the point are some of the proposals that are rather routinely made at Carnahan and similar forums for further domestic wiring. A paper from Radiation Incorporated, a major electronic battlefield contractor, talked of and clearly advocated heavily sensoring American communities to keep an electronic vigil on golf courses, shopping centers, construction sites and the like. The author of the paper, Guy H. Smith Jr., created a mythical Smithville, U.S.A., with a population of 80,000 to 100,000 people, which he felt could be adequately taken care of with a collection of 1,100 assorted sensors. He ended his presentation by predicting that Smithvilles—each replete with an "environmental assessment center" for sorting out the blips—will be "very common" in the future.

This apparently does not seen too far-fetched to others because a conference paper given by a sensor expert from Sylvania talks of the need for police equipment that will routinely process the output of a thousand or more sensors. Other trial balloons launched at recent Carnahan sessions have included calls for citywide schemes for infrared and television surveillance and plans for electronically tracing the movement of vehicles and people.

ORWELLIAN IDEAS

When you get into the realm of proposed tracking schemes, there are some especially Orwellian ideas around. A prime candidate for

the most startling of all did not appear at the Carnahan conference but in a forum just as august, the journal Transactions on Aerospace and Electronic Systems. The article by Joseph Meyer, an engineer in the employ of the National Security Agency, recommends a system in which tiny electronic tracking devices (transponders) are attached to those 20 million Americans who have been in trouble with the law—in fact, wearing one of the devices would be a condition of parole. The transponders would be linked by radio to a computer that would monitor the wearer's (or "subscriber's" in the words of Meyer) location and beep out a warning when the person in question was about to violate his territorial or curfew restrictions.

In addition, these little boxes would be attached to people in such a manner that they could not be removed without the computer taking note of the act. Taking off or tinkering with your transponder would, in Meyer's world, be a felony. Good engineer that he is, Meyer has also thought out some of the other applications of these portable units, which include monitoring aliens and political minorities. Robert Barkan, the writer who first brought the Meyer proposal and other such ideas to a broader audience through his articles, had this to say about the transponder system in The Guardian: " '1984' is still fiction, but no longer *science* fiction. The technology of the police state is ready. All that remains is for the government to implement it."

Significantly, almost everyone who has looked into the domestic electronic spinoff from military surveillance technology comes back to "1984." Unfortunately, however, making comparisons to Orwell's classic does not seem to have quite the same horrific clout it had a few years ago. At the end of the International Security Conference in Washington in 1972, the conference coordinator, Art Lilienthal, made this telling comment to a reporter from The Washington Post: "There was a time when the public was very much upset about 'Big Brother!' Now, the public is beginning to accept this as a fact of life. They recognize, realize, appreciate and accept the fact that Big Brother is not really some alien being, but that he's their friend."

If this is true, then our choices are limited and it is just a matter of time until our options boil down to the extras we will take with our lawn sensors and the color we will choose for the transponder that hangs around our neck. If not, there is still time to heed the implied warning of Orwell's vision as well as other more recent warnings. An appropriate one was a little-noticed caveat that appeared in a 1967 paper of a Rand Corporation systems engineer, Paul Baran, with experience in military and police command and control systems. His thesis is that while new equipment and techniques are needed by law enforcement agencies, it would be easy to go too far and make it too easy to gather information on individuals, which would lead to an intoxication of power, which, in turn, could pave the way for ". . . the most effective, oppressive, police state ever created."

Nearly 10 years have passed since Baran's warning, and all the arrows point to the conclusion that it is now more relevant than when it was originally issued. This seems to be so not only because of the tons of electronics gear installed to watch over America in the interim, but also because of the continually remarkable pace of technology.

At the time of the Baran paper, today's most effective surveillance instruments were only imagined. An important representative ex-

ample of what has since been created is a special TV camera for the surveillance market that was announced by the General Electric Company in 1974. It is remarkable on two counts. First, because of its ability to take crisp pictures with no more light than that given off by a single candle, it stands as the world's most sensitive TV camera. Second, it is wallet sized and weighs less than a pound. For the snoopers, the privacy-shattering potential of just this one piece of hardware seems vast.

[From the New York Times, July 27, 1976]

Olympic Fears Stir Border Patrol Shift

(By John Kifner)

Franklin, Vt.—A Border Patrol agent, Sterling Smith, his heavy silver and turquoise expansion watchband and cowboy boots marking him as a man of the Southwest, stood by the bright orange metal gate at the Canadian border, scanning the unfamiliar, densely wooded landscape.

"It's different up here," he said. "Down there we're always chasing. We've always got some Mexicans to chase."

Mr. Smith is one of 40 men from around the country pulled into this corner of the Northeast because of the Olympic Games, being held in Montreal, some 60 miles away. The reinforcements have roughly doubled the strength of the Border Patrol along the 174-mile stretch of Vermont and New York states known as the Swanton District.

The district encompasses the major routes to Montreal along Interstate 87 in New York and Interstate 89 in Vermont, along with Lake Champlain.

But it is the stretches of woods and fields and the countless tiny back roads and dirt tracks that wind through the back country along the border that are worrying the Border Patrol, rather than the formal entry points where checks are conducted by customs and immigration officials.

The major concern, said the chief patrol agent, John K. Lovejoy, who is in charge of the Swanton District, is that terrorists who struck the Olympic Games in Munich four years ago might attack the Olympics in Montreal and then try to escape across the border. The patrol is working closely with the Royal Canadian Mounted Police, which along with the Canadian military is imposing tight security on the Games.

As a result, Mr. Smith, an agent who normally works near Lubbock, Tex., is with other reassigned agents, checking places like Richards Road here, where the dirt track ends at the barrier, picking up again into a road on the far side of a Canadian farmer's buildings. Several years ago, the Border Patrol erected locked metal gates across these back roads to cut down on the illicit traffic.

Mr. Smith met up with Walter H. Massey, an agent detailed here from Orlando, Fla., to check on signals set off by the electric sensors, relics of the Vietnam war, that have been planted along the border. They had been set off by the wind.

Both men wore what they called the "river uniform" of dark olive work pants and Western-style straw hats rather than the more formal "Smokey Bear" hats and trousers with a dark stripe of the dress uniform.

"If you're chasing some 'wet' over a barbed wire fence and tear your stripe, it's really going to cost you," drawled Mr. Smith, using the patrol slang for wetback, or illegal alien.

On Lake Champlain, where the Border Patrol operates a water patrol out of Rouses Point, N.Y., Jerry Joplin from Fort Stockton, Tex., was teamed with Darall Brown, a local agent, on a 22-foot Penn Yan runabout. All Border Patrol agents being their service on the Mexican border, and many know each other from their frequent transfers to duty stations around the country.

While the border with Canada, marked here by a highly visible 20-foot swath cut through the woods and fields is a peaceful and friendly one, the Border Patrol agents say the situation is far from quiet. An arm of the Justice Department, the Border Patrol has the mission of stopping illegal aliens from entering the country.

In this part of the country, Chief Lovejoy and other agents said, there are frequent attempts by aliens of various nationalities to sneak into the country and disappear into the ethnic communities of the cities of the Northeast. Often the agents hide out in the middle of the night—"lying in," they call it—to intercept cars or truckloads of aliens on the back roads.

So far this month, Chief Lovejoy said, agents in his sectors have apprehended 232 illegal aliens. They are sent back across the border.

A major problem, the agents say, is that, despite the gates on the back roads, the aliens can come in on foot and then be picked up later by professional smugglers, who sometimes get as much as $700 per person.

The deputy chief agent, Jack Gorman, found one such possibility the other day when he sighted trampled grass among the cornfields leading to a barbed wire fence at the border.

"We used to have guys who could put a hand down and say, 'This was a 200 pound man with brown shoes,'" said Mr. Gorman as he studied the tracks.

"Why do they come?"

"You could consider it a form of flattery," said senior patrol agent Harry Van Leuvan. "The United States has a way of life no other country has. It's still the land of opportunity."

[From the Washington Star, July 25, 1976]

Moss Claims U.S. Wiretaps On Increase

FORD TOPS NIXON IN REQUESTS TO AT&T, PANEL CHIEF SAYS

The chairman of the House investigations subcommittee said today the Ford administration has asked American Telephone & Telegraph Co. to install many more wiretaps than the Nixon administration did.

"We've seen a marked, dramatic increase under Ford," declared Rep. John Moss, D-Calif. "Who is he tapping? Why the escalation?"

Moss made the statements as AT&T officials refused to give the subcommittee their records of the government's national security wiretap requests. They acted in accordance with an order issued yesterday by U.S. District Court Judge Oliver Gasch.

The judge's temporary restraining order represented a victory for President Ford, who had asked the Justice Department to "undertake such action in the courts . . . as may be appropriate to prevent the disclosure of this sensitive information."

At the White House, Press Secretary Ronald Nessen said he would have no comment about Moss' statement. "It's in litigation, I just can't comment," Nessen said.

Moss said a Justice Department affidavit outlining its wiretap requests to AT&T shows 76 in 1972; 95 in 1973; 141 in 1974, with 115 of them after Ford became president in August; 141 again in 1975 and 58 for the first six months of this year.

There was no indication whether the requests came from Ford himself or from others in his administration.

Moss criticized Gasch's temporary restraining order barring AT&T from giving up its records including more information about the wiretaps. The congressman also criticized Ford's request for the order.

"The President is charged with seeing that the laws are faithfully executed," Moss said. "Rather than carrying out his responsibility, he is interfering with the legislative powers of the congress enumerated in . . . the Constitution."

In refusing to turn over company records, John Fox, vice president of AT&T, told the investigations and oversight subcommittee that the firm would not risk being held in contempt of court by complying with the panel's subpoenas.

Moss temporarily excused the company from complying with the subpoena but added that this "in no way absolves AT&T from its ultimate responsibility."

The congressman said the President's request for the judge's order "flies firmly in the face of every historical precedent." He said Congress will resist any attempt to make Gasch's order permanent.

Ford's claim of executive privilege was only the second time a president has made such a formal assertion in an attempt to keep information from a congressional investigating committee, the Justice Department said.

In the first instance, an appeals court in 1974 upheld then-President Richard M. Nixon's refusal to turn over White House tapes to the Senate Watergate committee.

Judge Gasch has set a hearing July 28 to consider issuing a permanent injunction barring AT&T from turning over its wiretap records.

The 11th-hour restraining order was requested by Rex E. Lee, an assistant attorney general in charge of the Justice Department's Civil Division, at Ford's request.

Lee told Gasch that this was a "rare case, only the second time in history where the president has asserted executive privilege in the subpoena of documents by the Congress."

The court action followed weeks of unsuccessful negotiation between the White House and Moss in an effort to resolve the issue. The purpose of the House investigation is to determine the extent of illegal

wiretapping done by telephone companies at the request of law enforcement and intelligence agencies.

The subcommittee wants to find out how wiretapping may be violating provisions of a federal law designed to guarantee privacy in all communications, whether by wire or radio.

Ford, in his letter to Moss, said, "I fully understand your desire for some procedure by which you can obtain information relevant to your inquiry," but that the subpoena presented "unacceptable risks" to national security.

He presented as an alternative a plan under which the FBI would separate documents held by AT&T relating to domestic telephone surveillance from those dealing with foreign intelligence surveillance and provide the former to the subcommittee.

Under Ford's offer, foreign intelligence documents from any two years also could be obtained by the subcommittee, but they would be "edited" to delete "names, addresses, line or telephone numbers and other information which would disclose targets of the surveillances, sources of information about the targets, and methods of surveillance." The documents would disclose, however, whether the targets were U.S. citizens.

Lee argued before Gasch that if the unedited letters were sent to the subcommittee, the surveillance targets would become known.

Lee contended in papers filed with the court that such disclosures "would terminate various intelligence and counterintelligence programs, would identify and endanger informants and double agents currently supplying intelligence and counterintelligence information to the United States, would reveal the technical capabilities of the United States in obtaining such intelligence information, would eliminate valuable sources of information important to the national defense and national security and would severely hamper the conduct of our relations with foreign powers."

The Justice Department official argued that the Supreme Court in the Nixon tapes case noted the special need to defer to executive privilege in national security matters, especially where alternative methods of obtaining the information were available.

He added that this case was unique because the documents sought were in the possession of a private company and not the government.

"The government must rely on private industry for many needs, such as defense equipment, since it does not have the capability to provide the material itself. The situation here is the same: AT&T performs a function that only they can perform," Lee said.

He contended that the letters were sent to AT&T under a requirement that they be kept confidential and that AT&T must keep them secret. Lee noted that such letters only have been sent since 1969 and that before then the surveillance requests were made verbally.

[From the Washington Star, July 25, 1976]

Hill Unit To Appeal On Wiretap Logs

A House subcommittee announced yesterday it will appeal a federal court decision supporting President Ford's refusal to provide the

panel with telephone company records of national security wiretaps.

Chairman John E. Moss (D-Calif.) of the Interstate and Foreign Commerce subcommittee planned to follow up the formal notice of appeal with an affidavit Tuesday urging the U.S. Circuit Court of Appeals to rush a decision on the case—believed certain to reach the Supreme Court.

A subcommittee staff member said Moss views his legal battle with the President as "a kind of classic constitutional confrontation" involving the conflicting claims of executive privilege and congressional prerogatives.

Moss said his Subcommittee on Oversight and Investigations must determine whether the executive branch is using the warrantless wiretaps for legitimate foreign intelligence surveillance. All other kinds require warrants.

Mr. Ford decided two weeks ago it would be an "unacceptable risk" to turn over records that might enable 435 House members and their staffs to see in one place the names of U.S. agents, double agents and informants.

[From the Washington Star, Aug. 1, 1976]

'Less Than Candid'

Moss Criticizes Justice on Wiretaps

(By Stephen V. Aug)

The chairman of a House subcommittee, citing apparent discrepancies in figures concerning the number of wiretap installations, has accused the Justice Department of being "less than candid" with Congress and the courts.

Rep. John E. Moss, D-Calif., chairman of a House Commerce investigative subcommittee whose investigation into the propriety of national security wiretaps has been frustrated by a federal judge, said that only one of three people at the Justice Department may be giving correct information about the number of wiretaps. The three are Atty. Gen. Edward H. Levi, James B. Adams, assistant to the director of the FBI, and John K. Russell, a Justice Department publicist.

Moss said that an affidavit by Adams filed July 21 in U.S. District Court here said that in 1974 there were 141 letter requests for wiretaps to all telephone companies.

Levi, however, wrote the House Judiciary Committee on June 24, 1975, that there were 190 installations in 1974, and repeated the same figure to a Senate committee last November.

Russell said a week ago that since mid-1974 one request letter covered only one target, instead of one letter covering several targets, which was sometimes the case in earlier years.

"But if Russell is correct," Moss said, "then either Adams or Levi is wrong. Moreover, in his testimony before the Church committee (Sen. Frank Church, D-Idaho, who is chairman of an intelligence subcommittee), Levi added that the 190 installations covered 148 subjects.

This still conflicts with Adams' affidavit and contradicts Russell's statement that one letter equals one tap.

"There is simply no way to square all these statements. It seems that either the attorney general has misled the Congress and the public or that FBI official Adams has misled the District Court."

Moss contended that there was another apparent conflict dealing with 1975. Adams had said that 141 request letters were sent in 1975. Levi testified that through Oct. 29, 1975, there were 121 telephone wiretaps. Russell said that for the entire year there were 122 taps.

Moss said that Adams' affidavit gives figures that are both higher and lower than previously-issued official figures.

Moss' subcommittee has jurisdiction to investigate nearly all federally regulated agencies, and the wiretap investigation is being justified on the grounds the subcommittee's jurisdiction extends to the Communications Act of 1934, under which telephone companies operate. The law provides for secrecy of communications.

The subcommittee last month issued a subpoena to American Telephone & Telegraph Co. for documents concerning electronic surveillance requested by the FBI. The bureau and its parent, the Justice Department, objected to AT&T's complying with the subpoena on grounds there could be disclosure of sensitive national security information.

After weeks of negotiations, Moss and Asst. Atty. Gen. Rex Lee reached an agreement under which the subcommittee would be able to examine the requests under certain limited circumstances. The agreement, however, was never signed because of objections from the CIA and others in the intelligence community.

U.S. District Judge Oliver Gasch issued a temporary restraining order a week ago, and made it permanent Friday night, forbidding AT&T from complying with the subpoena. Gasch agreed with the Ford administration that Moss' investigation would involve unacceptable risks of disclosure of extremely sensitive foreign intelligence and counterintelligence information.

[From the Washington Post, Aug. 8, 1976]

The Computer as Couch

(By Eric Shulman*)

Like most people, I have always regarded myself as at least passably sane, beset by no more than a fleeting dozen or so hangups. Unlike most people, I have now been reassured by Control Data Corp.'s Model 3200.

A computer gave me a battery of psychological tests, flashing hundreds of questions on a video display terminal and digesting into its memory banks the answers I keyboarded back. Then, whirling along at the rate of 700,000 operations a second, Model 3200 interpreted the results and issued a printout with an instant diagnosis of the state of my mental health.

*Shulman is a free-lance writer and documentary film producer in Los Angeles. This article is reprinted from Human Behavior magazine.

"The patient," reported Model 3200, greatly to my relief, "is essentially within normal limits." The computer next spewed forth insights it had gleaned into my personality, concluding that I tend to be on the non-assertive side but am "aesthetic, sensitive and socially perceptive."

The future is here. Psychiatric diagnostic tests administered by an on-line computer have graduated from the realm of fantasy and have become an integral part of the Salt Lake City Veterans Administration Hospital's clinical routine. Since September 1974, nearly 3,500 psychiatric patients have undergone this sort of automated analysis in a prototype program sponsored by the VA and the University of Utah Medical Center.

Every day, say program evaluators, the computer is proving itself a remarkably effective tool in guiding clinicians to the right course of therapy for each patient. For instance, a 21-year-old man with a history of depression and extreme anxiety had long baffled doctors. None of the usual causes and treatments seemed to apply in his case. Then the computer, spotting some critical inconsistencies in his test scores, suggested an examination for organic brain damage. Sure enough, that's what the doctors found.

A NEW AGE

The program is still in the experimental stage, but the people involved with it are convinced they have entered a new era in the application of computer technology to the behavioral sciences.

"We are not, of course, suggesting that computer terminals will replace clinicians in treating patients," says Dr. Thomas A. Williams, a soft-spoken 39-year-old psychiatrist who is coinvestigator on the project. "But we do think we are demonstrating that a computer can perform some valid functions in a mental health care delivery system, especially in the diagnostic procedure, and perform them with more efficiency and greater precision than attainable before. It can show you what to do more effectively—and the result is better patient care."

The computer's reliability is under continual monitoring and evaluation. One study focused on two groups of institutionalized patients—one group diagnosed by the computer, the second group by physicians—and asked treatment personnel such as nurses and therapists to assess the "correctness" of the initial workup. The computer beat out the physicians, 96 per cent correct to 83 per cent correct.

Located in the foothills of the Wasatch Mountains overlooking Salt Lake City, the hospital receives about 300 new psychiatric patients a month. The computer administers a battery of standard psychological tests to every incoming patient. Critical clinical decisions—for instance, whether to admit a patient to the hospital or go with outpatient care—are made on the spot on the basis of the findings that come flowing from the computer.

Not only is the diagnostic procedure speeded up—approximately five hours on the computer versus three to five days for a similar battery of tests administered conventionally—but also the massive amount of interactive analytic data seems to be producing more thorough and accurate diagnoses.

"We are getting a richer picture of our patients," says Dr. James H. Johnson, a 35-year-old clinical psychologist, the second co-investigator on the project.

FINDING OVERSIGHTS

Over and over again, Model 3200 is turning up things human beings missed. Such as the case of the middle-aged veteran, an alcoholic, who was headed for confrontive group therapy until the computer identified him as a paranoid schizophrenic.

Dr. Ronald A. Giannetti, the clinical psychologist who handled the case, recalls: "This particular patient had had multiple hospitalizations for alcoholism, but had never before been diagnosed as a schizophrenic. He was a quiet, withdrawn guy who didn't socialize much on the ward. Apparently, no one had really talked to him before.

"He was admitted here off shift, so we didn't see him at first. Confrontive group therapy, a common treatment for substance abuse, had been prescribed when we happened to pull him off the ward for the standard battery of computer tests. He came out as a classic paranoid schizophrenic. And confrontive group therapy is not what you want to prescribe for someone in that state. It can lead to a blowup—precipitate an episode. If it hadn't been for the computer diagnosis, he would have had confrontive group therapy. It could have broken the guy up. He would have gotten depressed and possibly suicidal."

The files of the Psychiatric Assessment Unit (PAU)—the formal name of the computer intake program—are replete with similar cases. One 46-year-old woman veteran was also an alcoholic and had checked in and out of hospitals for years for drying-out programs. Not until she checked into the Salt Lake City VA Hospital and was subjected to computer testing was there a deep probe behind the surface symptoms of alcohol abuse. The computer turned up a history of four suicide attempts and frequent cyclic mood swings. Diagnosed as having a severe depressive disorder, presumably the root cause of her alcoholism, the woman is now under therapy for depression, her prognosis regarded as good.

To some of us, the specter of a computer probing the inner reaches of the human mind can be downright eerie. And watching a patient's printout race ahead with its findings like so many stock market quotations—anxiety: marked; depression: moderate—does make one wonder if 1984 hasn't arrived a little early in Utah.

But Williams and Johnson insist there is no need to worry.

Seated amid a clutter of books, reports and printouts in his office adjacent to the computer room, Johnson leaned back in his chair and mulled it over for a moment. "Sure," he said, "we recognize that philosophical questions like that are being raised. But really there is nothing frightening or Big Brotherish about it at all.

"Essentially, what we've done is to take the same type of common, proven psychological assessment tests used for years and computerized the process. We've programed in scoring keys and standard interpretations and analyses of the scores. The only difference is that our patients take the tests with the computer instead of with paper and pencil and clinical interviews. And instead of waiting days for the tests to be scored and interpreted, we get the results within 10 to 20 seconds after a patient completes the test battery."

QUICK DECISION

In most mental health situations, Johnson added, there is a critical decision that must be made at the onset. "One of three things has to be decided: whether the person needs help at all, whether the person can be treated on an outpatient program or whether the person requires hospitalization," he said.

"To perform that kind of diagnostic assessment, you normally hospitalize a patient for three to five days. Here, a patient who arrives in the morning can go home the same afternoon. Or, if the patient has to be hospitalized, a complete workup is in the hands of the treatment personnel immediately and treatment can begin all that sooner."

And, Johnson said, there is a big cost savings. With the conventional procedure of hospitalization for three to five days of testing, it costs up to $500 per patient for a complete mental health workup. The computer does the same job at an average of $120 per patient.

Aren't we running a risk of snap judgments and superficial labels being applied in the mental health treatment process—judgments and labels that can stigmatize a patient and frustrate the chances for recovery?

"I don't see that happening at all," Johnson replied. "For one thing, you're going to have the process of labeling with or without the computer. And if anything, the computer is reducing the risks because it is proving itself more accurate and definitive in its patient assessments. There is less likelihood of a wrong label to start out with.

"The second thing is that in our society the mere fact of being admitted to a mental hospital tends to hang a person with the label of mental illness. Other places are admitting people just to get them assessed, and they come out often with the label on them. The computer system permits us to do the diagnosis and the workup preliminary to admitting.

"It used to be that 75 per cent of the people who showed up here for some kind of mental health help were admitted. Many of them were admitted just so we could find out there's nothing seriously wrong with them. Now the number admitted is only 45 per cent. The computer enables us to determine what's wrong with people without having to institutionalize them. We're finding a majority can be treated effectively under out-patient care or in some kind of referral care. So the use of the computer reduces the number of people who may become labeled as patients of a mental institution.

"Another thing about this business of labeling—which is a big controversy in the whole mental health field—is that the computer printouts contain both a diagnosis and a problem list. For those people who believe in a diagnosis and who treat with chemotherapy, we provide a diagnosis. And for those people who believe in the behavioral therapies, we provide a problem list."

When new patients enter the two-story building housing the PAU, they are met by a receptionist with a computer terminal next to her desk. She programs in each patient's name, social security number, chief complaints and other pertinent data.

Then each patient is assigned to one of the 10 video display terminals scattered in brightly decorated test and interview rooms on the first floor and begins taking the basic, or core, battery of six automated diagnostic tests.

First comes Questionnaire One (Q-1)—a brief, five-minute true-and-false test developed by the PAU to assess the patients' ability to understand the test procedure and their likeliness to answer truthfully. Results are printed out in the computer room upstairs.

Other tests in the core battery are:

The *Minnesota Multiphasic Personality Inventory* (*MMPI*)—a basic and widely used psychological diagnostic tool that has been refined to a pool of 566 questions in this computer program. Each question flashes individually on the screen, the patient keyboards back either true or false and then punches a "return" button to order up the next question. Results are printed out in the form of raw scores on the 13 standard clinical and validity scales incorporated into the *MMPI*. A profile graph is also printed by the computer, along with a narrative interpretation of the findings and a list of critical items.

Shipley-Hartford Intelligence Scale—has been refined to 60 items covering verbal and abstract ability. The computer prints out raw scores, an equivalent IQ and any critical mistakes.

The *Beck Mood/Hopelessness Scale*—another commonly used paper-and-pencil examination adapted to the computer, measures depression level and suicidal intent. The computer reports a raw score and a brief narrative analysis with statements such as: "This score suggests that the patient is not experiencing a depressed mood." The computer also prints out critical items. If, for instance, a patient has answered "true" to question 19 ("I have lost more than 15 pounds"), the computer will note that under critical items.

The *Current and Past Psychopathology Scale* (*CAPPS*)—is an automated mental status exam that, unlike the other tests, is not self-answered directly into the computer by the patient. Paraprofessional interviewers, mainly psychology graduate students from the University of Utah, administer this test, prompted by questions appearing on the video display terminal. The test consists of some 209 items covering history of childhood and adult symptoms, affect and mood, delusions and hallucinations. The computer has been programed to "branch" for this test, tailoring sets of questions to the individual patient. Fo rexample, if a patient reports his or her parents were divorced when the patient was a child, the computer will branch into preprogramed questions focusing in on that aspect of social history.

A computer-prompted physical examination—a paraprofessional administers a basic physical examination (respiration rate, psychomotor reflexes, medical history and so on) and programs in the results. Again the computer can branch, suggesting other items to probe for on the basis of prior responses.

LODE OF DATA

In its printout, the computer will yield up a wealth of data, noting among other things any neurotic and psychotic symptoms, measuring the severity of illness on a standard scale, pointing up any critical inconsistencies in the test scores and enumerating a problem list to guide subsequent therapy. The paraprofessional workers, trained to interpret the printouts, decide whether to admit patients to the hospital or assign them to an out-patient program or whether the findings rule out the need for any treatment. For unusual cases, a clinical psychologist and a social worker are available for consultation.

The use of computer technology in the behavioral sciences is, of course, hardly new. Computers have been used for years in data processing for research and for health care program administration. There have also been a few other experiments in clinical use. But the Salt Lake City program, funded by $500,000 in grants from the VA and the National Institute of Mental Health, with the computer hardware donated by the University of Utah, is the most elaborate undertaken and the only one that has put thousands of human beings into an online interface with a computer programed deeply to probe their personalities and mental status.

How does automated analysis sit with the people on the receiving end, the patients themselves? Quite well, judging by the results in Salt Lake City.

One psychologist, Daniel Klingler, has been conducting a series of independent evaluations of the computer's effectiveness and of patient reaction for the University of Utah. He has found that, for the most part, patients actually prefer the computer to conventional interviews and paper-and-pencil testing. In one study of 132 patients who had gone through both processes, 89 percent said they favored the computer and 78 per cent said they did not find the computer "too impersonal." Fifty-six per cent said they were "more truthful" in answering conventional tests, and 45 per cent said there was no difference in their truthfulness.

FRIENDLY KEYBOARD

No one has any definitive answers yet as to why patients seem to prefer "talking" to a computer over a human being; but the people at the PAU like to speculate on that subject. Johnson believes the entire process, filled as it is with lively interaction of questions moving across a screen and the need to keyboard back responses, becomes a stimulating and gratifying experience to many patients, Klingler believes that in some ways the computer actually appears to be less impersonal.

"I don't think it's as threatening to some people as sitting down with a shrink," Johnson says. "There is no social stigma attached. There is more feedback. The extent of the testing, all concentrated into a relatively brief period of time, seems to say to a patient that somebody really cares. They don't get this impersonal feeling of 'Call me next week.'"

In a startling by-product of the PAU program, the researchers are even finding some cases where the computer questioning seems to be taking on some of the therapeutic aspects of analysis. Answering one of Klingler's questionnaires, a patient wrote: "It opened my mind to things that has [sic] long been lost into history. In fact, I was quite surprised to be able to remember so far back until my childhood. I guess I just didn't stop to think about it until now." Wrote another patient: "It made me realize that nothing is wrong with me. I am just very, very sad over the death of my girlfriend, which is only natural."

Finally, there was the case of perhaps the most satisfied computer patient of all. This man, an out-patient, wanted to know if he could purchase a terminal to install in his home so that he could have a session with the computer whenever he felt low. That kind of reaction can be viewed as either encouraging or frightening, depending upon whether you own stock in IBM or in a couch manufacturer.

[From the Washington Star, Aug. 19, 1976]

C&P Puts the Arm on People Dialing 411 for Information

(By Mary Ann Kuhn)

The Chesapeake & Potomac Telephone Co. is out to catch those people who live and work in Washington and chronically dial 411, the telephone number for information.

Telephone operators are questioning people who call 411 in the city this week in an effort to learn where most of these "information" calls originate—whether from residential, business or coin-operated phones.

The information will be helpful whenever the company decides to go back to the D.C. Public Service Commission and ask for permission to charge District customers for information calls or directory assistance calls.

The way the company is going about this querying, which began Sunday and continues through Saturday, has irked a few 411 dialers.

First, the caller gets that nearly two-year-old recording that slashed from 350,000 to 230,000 the number of information calls daily in the metropolitan area:

"The number you want may be in your directory. Would you please check. If you need help, wait for an operator to answer."

Then the operator answers. The caller asks for a certain number. Before she gives it out, she snaps: "Are you calling from a business, residence or coin-operated phone?"

In one case, a customer who refused to disclose that the call was coming from a residence, was turned over to another operator, who finally gave the number requested. The person calling from the residence didn't have to say where the call originated from.

The caller didn't know it but a computer was automatically recording the exact address of where the call was coming from anyway, according to a company spokesman.

"There is no attempt to harass a customer," said Web Chamberlin, spokesman for the telephone company. "I can't say it's not happening. But the project is not designed to harass customers."

Chamberlin said the company has reported "no significant number of complaints" from customers. "If customers object, we give them the information and move on."

Telephone officials feel that the information they get from the survey will be a point in their side when they go before the Public Service Commission to ask for a charge on directory assistance calls in the city.

The company hasn't decided when it would make that request, a spokesman said. The last time it did, the company was turned down. It had sought approval from the PSC to allow callers three free information calls each month, and any more after that would cost the caller 20 cents apiece. There were exceptions for handicapped persons.

But the Public Service Commission rejected the request in May when it granted the company an overall $7.4 million rate increase. One of the reasons was that the commission didn't feel the company had given enough information, such as calling patterns of people, and other evidence to back the request.

In Virginia the C&P Telephone Co. will begin charging 10 cents for each call for directory assistance after six such calls per month, starting Nov. 6.

In Maryland there is a one-year moratorium on directory assistance charging. Gov. Marvin Mandel signed a bill to that effect at the last legislative session.

There are 15 areas—states and localities—where the Bell system charges for directory assistance, according to Chamberlin. They include the states of Wisconsin, New York, Georgia, South Carolina, North Carolina, Illinois and Colorado. Cincinnati also has it.

Charging its customers for information calls "is not designed to provide revenue to our company," said Chamberlin. "Our attempt is to drive the cost of service down so the expenses of the company are less."

[From the Washington Star, Oct. 25, 1976]

A Former Spy Tells of Being Left in the Cold

Agents in trouble callously treated, he asserts

(By William Beecher)

Bruce Taylor Odell is a spy who was left out in the cold.

For nearly 20 years Odell, a 48-year-old native of Wellesley, Mass., worked in a variety of clandestine operations for the CIA.

Five years ago, he was eased out of the CIA on partial disability. By that time he had long since lost his respect for some of his superiors and was bitter.

Now Odell, who approached the Boston Globe, wants to tell his story in order to focus public attention on what he insists are abuses of commission and omission in the intelligence system, to spur reforms.

He is angry about what he says is callous treatment of operatives in trouble, giving rise to morale problems which undermine the CIA's ability to perform. And he worries about feckless officials who went along with political requests to get the agency involved in questionable operations at home.

The disenchantment of Odell began in earnest on July 21, 1965. At the time he was the No. 2 CIA man in Cairo, one of whose principal missions was to serve as the sub rosa contact through whom Egyptian President Gamal Abdel Nasser could pass sensitive information to Washington, without going through leaky diplomatic channels.

Odell says that sort of channel had been open for some years before he was posted to Cairo the previous August and that his name had been passed to Nasser in advance of his arrival. Actual contacts were not with the president, Odell says, but with Mustafa Amin, an Egyptian editor and close Nasser confidant.

But in the summer of 1965 it appears that Egyptian intelligence became suspicious that Amin was not only passing approved information but more, much more. His Cairo home was bugged, apparently with high quality eavesdropping devices provided by the United States for use against the Russians.

Odell suspects that the Russians had figured out his real identity, from previous covert operations, in Cairo, Tehran and Baghdad, and had persuaded Egyptian security that he and Amin were engaged in anti-Nasser espionage.

Odell's cover was that of political attache in the embassy, ostensibly as a Foreign Service Reserve officer.

On the day Odell's life and career began to unravel, he was to have lunched with Amin at the latter's summer place in Alexandria, a meeting set up one week before in Cairo. The meeting had been set for 2 p.m., but Odell arrived 40 minutes early and was having a beer and taking notes of a conversation with Amin when, at 2 o'clock sharp, more than 20 men, all armed, burst into the Amin garden and arrested the two men.

Odell's jacket was draped over a nearby chair; it contained his diplomatic passport. "I was standing at that point," he recalls. "Just as I reached for my coat, I happened to glimpse a reflection in the sunglasses of the man in front of me that someone was swinging at the back of my head. I dropped my right ear on my right shoulder." The blow to his left ear permanently damaged his hearing.

For about 2½ hours Odell says he was interrogated. They studied his elliptical notes. "Who's R?" he was asked. Actually the letter R stood for Nasser, but Odell says he gave no answers, just kept insisting that the American ambassador be called.

"By the time I left, there were all kinds of screams coming from upstairs," he says. "I didn't have to fantasize what was going on up there."

He drove to the American consulate in Alexandria and immediately wrote cables to Washington detailing what he had been told before the raid occurred, and what happened after. But the consulate refused to send the cables. "We don't want to alert the Egyptians," he was told.

His boss, the CIA station chief, happened to be in Alexandria at the time supervising a "black bag job," a break-in for intelligence purposes. But Odell says when word was passed, the station chief refused to see him or authorize transmission of his cables.

"This was so unbelievable," he says in retrospect.

He stayed for about two hours arguing, but to no avail. He was in the middle of a colossal flap and no one wanted to have anything to do with him. It was as if he had suddenly contracted leprosy.

Giving up in disgust, Odell asked that somebody accompany him to his beach cottage in nearby Agami, to protect him, his wife and their three children. He was told that no one could be spared then but that someone would contact him at 10 p.m.

"The only thing I can remember about the drive to Agami was that I was fantasizing what could have happened to my family." But the family was all right. He informed his wife, Ann, of what had happened, and then "burned everything that even looked like a U.S. government document in a bucket."

Ten o'clock came and went; nobody appeared from the consulate. It appears by that time that Odell was hurt, frustrated, worried and very angry.

He went across the beach to the house of a British official, also on vacation. He then did something for which some senior men in the

CIA and the State Department never forgave him. He wrote a blistering message for the American ambassador, Lucius D. Battle, with instructions that it be transmitted through the British ambassador in the event something happened to him.

What did the message say? Even now, more than 10 years later, Odell cannot suppress his bitterness. "The tenor of the message was, Mr. Ambassador, you don't have a ——— team here at all, you've got a bunch of scared, frightened pansies. Get their asses home."

The next day he drove with his family back to Cairo. Until that moment, the only information Washington had on events of the previous day came from the official Egyptian news agency, charging that Odell was a CIA spy working "under the guise of an attache." Amin, the report continued, had been arrested "while giving a weekly report at the request of CIA" to Odell.

Shortly after Odell got back, he says Nasser sent over Mohamed Heikal, a newspaper editor and close friend, with the message that he should leave the country at once. Odell was packed off on the next plane, leaving behind his distraught family. He says his wife soon thereafter received a personal call from a top embassy official with the curt message: "You can expect no special support from your husband's organization."

Odell notes: "At that point, her support disappeared."

Mrs. Odell sold some household furniture and the contents of the liquor cabinet to American newsmen to help finance the trip home.

Why would the government turn its back so coldly on one of its own? Why, indeed, especially since from his first training class he and others like him had been assured that in extremes they would be taken care of, and so would their families.

Odell says he spent the next six years inside the CIA trying to piece the answer together. His conclusion: Ever since the abortive Bay of Pigs operation, the predominant instinct of many CIA officials when a flap arose was to first protect their own careers and second the image of the CIA.

He insists he has seen too many cases like his own where CIA friends, associates and superiors would shun anyone unlucky enough to suffer public exposure or a failure. They simply became expendable.

The day after Odell returned to Washington, he says, he was called into the State Department and told he would be served up at a press conference the next day. He was told to stress that he was a Foreign Service officer, not a spy. But Odell was hardly in the mood; he apparently scared the diplomats with the graphic description of the arrest scene which he said he was prepared to tell. So he was not put through the ordeal.

Instead, State Department spokesman Marshall Wright told reporters: "He (Odell) was a political officer, an attache with the embassy, and still is.

"Very many U.S. diplomats know Amin . . . an internationally known publisher and journalist. It is completely understandable and normal that American officials would be in touch with a person of Mr. Amin's reputation. Contacts between American officials and Mr. Amin had been entirely open and above board."

Amin, by the way, was jailed for 10 years, receiving a pardon only last summer from Nasser's successor, Anwar Sadat.

And when Odell left the CIA, he was told to continue to maintain the State Department cover. He was sternly warned not to whisper his CIA connection to a soul; but if it did slip out, he was ordered to immediately report to the CIA the name of anyone aware of his true intelligence past.

That order, Odell has decided to disregard.

[From the Washington Star, Oct. 26, 1976]

Poor Morale, Image, Leadership

A Former Spy Sees a CIA Grown Ineffectual

(By William Beecher)

In the summer of 1963 the United States was determined to help the new government in Iraq, which had come to power in a coup after Communists had been named to a number of top military posts.

The Soviet Union reacted by cutting off arms aid. Iran and Israel compounded the new regime's problems by stepping up their aid to the rebellious Kurdish minority in Iraq.

The United States wanted to help the new government, but discreetly.

One night in August, a fleet of unmarked transport planes swept onto the Air Force base at Dover, Del., loaded up with tanks, ammunition and guns, and headed out before dawn. Their destination: an isolated airstrip in Iraq.

It was a covert CIA operation, smooth, quiet, efficient. Bruce Taylor Odell, a CIA Mideast specialist, was dispatched for three months with a special team to assist any way they could.

Odell is proud of how the CIA pulled off that mission and of his role in its success. He thinks it represents the kind of thing the CIA once could do very well.

Now, because of morale problems in the ranks, damaged public confidence, and what he insists is poor leadership, he questions whether the CIA today can perform effectively.

Odell, a retired veteran of nearly 20 years in CIA clandestine operations, has blown his cover in order to come forward and bear witness to some of the problems he says must be corrected.

Unlike some other disaffected CIA agents, he does not want to tear down the organization, publicize the names of any operatives or jeopardize current secret operations or capabilities.

On his last working day at CIA headquarters in Langley in late December 1971, Odell removed two mottos from the wall behind his desk. One said: "Don't assume." The other: "I give a damn."

Those two mottos sum up as well as anything what Odell stood for during his CIA career and why he left.

Odell at 48 does not fit the stereotype of a secret agent. He is 5 feet 10, bespectacled, balding, with laugh lines around his eyes and deep furrows in his forehead. His once lean frame now sports a pot belly, in part explained by the fact that rigorous exercise is forbid-

den because of some injuries incurred in 1965 when he was arrested and beaten by Egyptian secret police.

He knows and enjoys good food and wine, books, younger, un-motherly women, jazz, dancing, sailing and conversation. Three days and nights with Odell provided ample demonstration of how he must have worked recruiting agents in the field.

A natural raconteur, Odell is funny, charming, warm, ingratiating. But when his thoughts turn to darker subjects, it looks as if he could be mean, tough, ruthless.

Odell got into the intelligence business almost casually.

In the summer of 1951, he had just received a degree in economics from Queens University in Ontario, Canada. A professor suggested that he join the CIA.

"I'd been in Canada for five years," Odell says. "I didn't know who the hell the CIA was."

After trying the CIA and being turned away, he joined the Army, serving for three years.

But once the CIA had been contacted, it did not lose track of Odell. He recalls that every time he finished another course in the Army, a CIA man would show up to talk to him. One of them suggested he go to Anchorage, Alaska, and study Russian.

But Odell refused; he liked the Army. He went to OCS and became an officer. He considered making it a career, but recalls about that time the Army-McCarthy hearings started, and he soured on the idea.

A CIA man appeared at his Army headquarters one day and talked him into joining the agency. He did, accepting an appointment in September 1954 for a starting salary of $4,205.

After signing in he was polygraphed and then began an intensive, nine-month course in clandestine operations. He was interested in the Mideast and was initially assigned to the Iran branch. There followed several months of language training in Farsi, the Iranian tongue.

After a number of inside jobs at CIA headquarters, he was picked for the Iraq operation, where he earned a glowing commendation from the U.S. ambassador.

There followed an assignment associated with the military and field operations in Iran and Egypt—the latter two under State Department cover. It was in Egypt, in 1965, that his cover was blown and where the CIA, in his view, then treated him as expendable.

Back in the United States he was confused, angry and physically and mentally hurting. He took a sabbatical at Harvard beginning in August 1965.

The following summer, Odell was brought back to CIA headquarters to work in the Technical Services Division, which supports CIA operations worldwide. It provides agents in the field everything in the way of sophisticated bugging devices, radios, invisible inks, codes and weapons that they need to do their jobs.

Being back in headquarters at an upper-middle rank and a "need to know" about all operations all over the world, Odell had a series of eye-opening experiences. And he didn't like some of what he saw.

He recalls an incident when an outside inventor brought in an extremely small, but potentially revolutionary, communications device. But funding was denied, he asserts, because of bureaucratic

jealousy. The project had not come through the Research and Development office, and he claims the man in charge did not want credit to go elsewhere.

Odell says he witnessed several instances in which CIA men with brilliant records were cast aside the first time they got involved in a flap, as he had almost been after the Egyptian incident. He is convinced the reason for such callous treatment was the desire of certain senior officials to let nothing endanger their own advancement, regardless of the price in human terms and morale.

He was incensed when the CIA, despite the law forbidding it to get involved in domestic operations, acceded to White House pressure to actively support the spying on antiwar groups.

"And we were prepared to cooperate in the Huston Plan," he says, "which I can describe as nothing less than fascism." That was a plan to have all of the intelligence agencies, including the CIA, FBI and National Security Agency, coordinate efforts to spy on anti-war groups in the United States. The program was not implemented only because then-FBI Director J. Edgar Hoover refused to get involved.

"I saw ineffectiveness," Odell says. "I saw inefficiency. I saw diseconomies of massive scale.

He recalls the time when it was discovered that the military liaison office at the National Security Council had been duplicating secret papers of Henry Kissinger and forwarding them to the chairman of the Joint Chiefs of Staff.

Kissinger was so furious, Odell says, that he insisted the CIA come up with some way of making it impossible for such papers to be duplicated in the future. Odell put together a team that spent months on the project, finally succeeding. He won't say how. But he insists the project was a big waste of time and money.

Odell did not hide his unhappiness. He made a lot of enemies inside the CIA. He was in the process of getting a divorce when the CIA suggested he might want to resign. He refused. Then the agency suggested retirement of medical reasons and awarded him only $12,000 annually in retirement benefits.

Odell went home to Wellesley, Mass. He worked as an independent management consultant and even started his own firm, which collapsed with the business turndown in 1974. He sold insurance. He got involved in local politics.

Odell says he wanted to go public before. He had hoped that out of the intelligence community investigations of the Church and Pike committees that necessary reforms and changes in some top management would result.

He feels the congressional committees were "snowed," at times lied to.

"How come they never located and called on guys like myself who knew precisely what the mail-intercept operation was all about?" he asks. "I'd tell them in executive session. There was some perjury on that one."

At the end of three days of talking to a reporter, Odell was exhausted. On one occasion, in reliving the arrest in Egypt and its bitter aftermath, Odell had broken down into sobs.

But at the end, he was smiling. He was relieved that after so many years of holding back, he had let it all hang out.

"Hey, baby, he said, "I haven't felt this cool in a long, long time."

[From the Washington Post, Oct. 11, 1973]

Electronic Warfare Is a Major Factor in Mideast

(By George C. Wilson)

The dark art of electronic warfare—so secret that little is written about it—will help decide who wins this latest Arab-Israeli war.

The war communiques from both Cairo and Tel Aviv do tell that Egypt's missiles are pitted against Israel's planes in the battle for the Sinai desert, with losses of Israel's "flying artillery" of utmost concern to Tel Aviv.

But the communiques cannot describe the grim but silent struggle as technocrats on both sides try to give their fighting men the upper hand with modern weapons that can mean the difference between victory and defeat.

And how this part of the war comes out will provide a fresh measure of the relative merits of Russian and American weapons—a crucial measurement in this age when each superpower is hostage to the other's military might.

Egypt is counting on its Soviet-made and anti-aircraft missiles—the SA–2 Guideline, SA–3 Goa and SA–6 Gainful—to offset Israel's American-made F–4 and A–4 fighter-bombers as well as some French-supplied aircraft.

Israel is counting on tactics and electronics to keep Egypt's missilemen from knocking down too many of its planes so it can carry out its war plan to rely primarily on firepower from the air.

The SA–2 for high-altitude shooting and the SA–3 for low altitude have been around for so long that Israel has armed itself with electronic counter measures (ECM) to foil them, as did the United States when it came up against the SA–2 in Vietnam.

But the SA–6 is a newer anti-aircraft missile, although Russia paraded it as far back as the May Day Parade of Nov. 7, 1967. So the most challenging part of Israel's ECM battle is foiling this SA–6, an improved version of the low-altitude SA–3.

Starting with the fundamentals of electronic warfare, the "eyes" of today's modern missiles are radar. One type, called acquisition, goes out a long way to search for an invading aircraft and "acquires" it in the form of a blip on a radar scope. Another type tracks the plane and a third guides the missile fired at it—the fire-control radar.

Two basic techniques for fouling up these radars are to fuzz up the gunner's radar screen—like blurring a home television set—or to make the blip he is tracking appear far from its actual location.

But to perform these and lots of other electronic cat-and-mouse tricks effectively, the invader must know a lot about the radar being used against him—such as frequency, power level and width of the pulse.

Israel—and the United States—know those things about the SA–2 and SA–3. Collecting such electronic intelligence (ELINT) was the mission of the USS Liberty, shot up during the six-day war of 1967; the USS Pueblo captured off Wonsan, North Korea, in 1968, and the EC–121 spy plane shot down by North Korea in 1969.

A standard technique is to tape record these radar signals from antiaircraft batteries so that specialists back in the laboratory can figure out ways to disrupt them. But, to do this, the enemy tracking and fire control radar must be turned on.

Modern nations for decades have been playing an electronic game of "chicken," such as flying planes at another country's air defenses, to provoke antiaircraft batteries into turning on their radar so the signals can be recorded.

But this game of chicken costs lives, with the USS Liberty and Navy EC–121 only two of many examples of men killed collecting ELINT.

Israel, if the SA–6 is indeed taking a toll on its aircraft as Pentagon specialists believe, now must collect more ELINT on the SA–6 and design electronic counter-measures against the weapon.

Diving down on an SA–6 battery to record its firing signals would be highly dangerous, if not suicidal, since the missile is shot from close-range like a bullet. Two less costly options are using drones—airplanes without pilots—or capturing an SA–6 and then operating it to unlock its electronic secrets.

Israel does indeed have drones—an adaption of the Ryan target drone made in the United States. The Israeli version is the Ryan 124–I. So that possibility is in reach.

Since the Egyptians apparently have taken the SA–6 with them across the Suez Canal on tracked vehicles, Israeli forces may capture one before long. The SA–2 and SA–3 are also mobile.

The vehicles carrying the antiaircraft missiles may find it hard going in the sands of the Sinai and stick to one of the three roads near the Egyptian landing site—making it that much easier for the Israelis to steal a missile.

Electronic warfare specialists said yesterday that the SA–6 seems to be more maneuverable than the SA–2 or SA–3. This would mean that the operator guiding the missile with radio signals could achieve more accuracy by adjusting its fins in flight. American pilots found that the SA–2 could not keep up with them as they dove sharply and took other sudden maneuvers—a shortcoming that helped keep loss rates down to 2 percent.

The fewer planes Israel loses to the SA–6 and other missiles, the fewer replacement aircraft the United States will have to send. So it is virtually certain that more American ECM equipment to foil the missiles will be in an early shipment of war supplies to Israel. The Soviet Union, will probably send more offsetting equipment to Egypt in hopes of winning the electronic war.

Another front in this grim but little noted war is around the Golan Heights where, informed sources say, Syria is using the Soviet-made SA–7 Strella—a missile which homes in on the heat from a helicopter or airplane engine after being fired bazooka-style by an infantryman.

[From the New York Times, Jan. 18, 1974]

Satellite Films Soviet Space Base

U.S. SURVEYING CRAFT TOOK PHOTOS OF ASIAN LAUNCHING COMPLEX AT BAIKONUR

(By Theodore Shabad)

An American resource-surveying satellite that has been orbiting the earth since 1972 has yielded photographs of the Soviet Union's secret space launching complex at Baikonur in central Asia.

United States Government agencies charged with the satellite program have not made a special point of announcing availability of photos of the major base for fear of antagonizing the security-minded Soviet authorities. But these and any other pictures of the earth's surface are publicly available on request.

The unusual photograph of the Baikonur complex, taken by the Earth Resources Technology Satellite from 560 miles altitude, was first displayed Jan. 9 in Defense/Space Business Daily, a Washington newsletter. The publisher, Space Publications, Inc., later also printed the picture in its two other newsletters Space Business Week and Soviet Aerospace.

SENSITIVE RELATIONS

A spokesman for the National Aeronautics and Space Administration said, in answer to inquiries, that it was obligated, as an "open, peaceful agency," to put all information from the ERTS satellite into the public domain regardless of the national security policies of particular nations such as the Soviet Union.

American relations with the Soviet Union in the space exploration field are particularly sensitive because the United States does not wish to jeopardize a joint manned space mission planned for 1975. The NASA spokesman said total disclosure of the earth resources pictures had been decided on after "long, agonizing debate" within the Government.

Users can purchase the satellite photographs of any part of the world from the Geological Survey's EROS Data Center in Sioux Falls, South Dakota, by specifying the geographical coordinates. EROS stands for Earth Resources Observation Systems.

A recent inquiry for photographs of the Baikonur area, east of the Aral Sea, at Lat. 46 degrees N. and Long. 63 degrees 20 minutes E., was fed into the data center's computer. It reported that two pictures were available, one taken Sept. 5, 1972, with 20 per cent cloud cover, and a better shot taken March 16, 1973, with only 10 per cent cloud cover. Both were described as of good quality.

It was the 1973 picture that was reproduced last week by the Space Publications newsletters, together with a detailed interpretation of various installations at the launching complex. They appear as dark spots against the light-colored background of the surrounding snow-covered desert.

OFF-LIMITS TO PUBLIC

The space complex, which stretches almost 40 miles east and west, is omitted from official Soviet maps and is off limits to foreigners and

the ordinary Soviet public. The center was shown to Presidents Charles de Gaulle and Georges Pompidou of France, presumably because of close Soviet-French collaboration in space exploration and other scientific fields.

Although named for the village of Baikonur, 173 miles to the northeast, the space complex was appointed by Western intelligence sources around 1960 as being much closer to the rail town of Tyuratam. The space photograph shows the central portion of the complex, with housing and other urban services, to be 15 miles north of Tyuratam, with which it is linked by a road and rail spur.

According to the photo interpretation published by Soviet Aerospace, one of the Washington newsletters, the Baikonur-Tyuratam complex has at least three large launching pads for manned space flights and related operations.

Roads and railroads project from the central town area to the pads. Soviet films of manned launchings have shown rockets being moved by rail to the launching pads while astronauts travel by bus.

[From the Washington Star, Thursday, Sept. 4, 1971]

NSA 'Ear' Target of Spy Probe

(By Norman Kempster)

With many members expressing skepticism about an official denial, the House Intelligence Committee plans to hold hearings soon on charges that the super-secret National Security Agency regularly intercepts telephone and cable communications from the United States to foreign cities.

Chairman Otis Pike, D–N.Y., said the hearings would begin as soon as the necessary staff work can be completed and members have time to do enough home work to be able to "ask intelligent questions."

At the committee's last official meeting before the August congressional recess, Lt. Gen. Lew Allen Jr., the Air Force officer who is director of the NSA, told the lawmakers that at the present time the agency is not monitoring the overseas telephone calls of Americans.

Pike said in a telephone interview late yesterday that he was not convinced by the denial. He indicated the committee also was concerned with possible interception of cable and computer communications in addition to telephone taps.

The committee's first round of hearings concentrated on the budgeting procedure of the CIA, NSA and other intelligence agencies. However, there were repeated hints of extensive NSA monitoring of communications, convincing Pike and his fellow members that the subject should be studied thoroughly as the focus of the committee's next round of hearings.

Sources familiar with U.S. intelligence operations have said the NSA has the technology to intercept telephone, cable and other communications traffic almost anywhere in the world.

These sources say the agency uses a sophisticated computer programmed to react to "trigger words" like "defense," "Russia" or any other word that probably would be contained in a conversation of in-

terest to U.S. intelligence. The computer separates messages of possible significance from the bulk of overseas communications.

Pike said he would confer today with Sen. Frank Church, D-Idaho, chairman of the Senate Select Intelligence Committee, to discuss the parallel investigations.

"There is more to be investigated than we have time to investigate so there is no need for duplication," Pike said.

It seems unlikely that Church would attempt to intrude on Pike's plans to probe the NSA. The Senate committee is winding up a three-month study of CIA involvement in assassination plots and it has announced that its next target will be the CIA's covert attempts to manipulate political events in other countries.

The Pike committee received apparently conflicting testimony last month on the subject of NSA monitoring of communications. CIA Director William E. Colby told a public session that the NSA does intercept "foreign communications," which could include the calls of Americans.

The NSA's chief lawyer said during a public hearing that in his opinion the agency has ample legal authority to monitor the overseas calls of Americans in spite of recent court decisions against wiretaps. But Allen later denied during a closed committee session that American telephone calls were being overheard.

Several members of Pike's committee have expressed doubts about the denial. Rep. Les Aspin, D-Wis., suggested after last month's hearing that information about NSA activities should be sent to the Justice Department for possible prosecution of violations of wiretap laws.

The NSA, once so secret that its existence was officially denied, has the responsibility of protecting U.S. official communications—generally through the establishment of code systems—and of breaking the codes of possible adversaries.

The agency has been kept so closely guarded that Allen complained last month his appearance before the Pike committee marked the first time an NSA director had ever been questioned in public by a congressional panel.

[From the New York Times, Aug. 30, 1975]

National Security Agency Reported Eavesdropping On Most Private Cables

Pentagon unit is said to use computers to sort out intelligence data from messages—legality is debated

(By Nicholas M. Horrock)

Washington, Aug. 30—The National Security Agency eavesdrops on virtually all cable, Telex and other nontelephone communications leaving and entering the United States and uses computers to sort and obtain intelligence from the contents, sources familiar with the operations said today.

The agency's operations make it privy to the inner workings of thousands of American and foreign corporations, the sources said, as

well as to the private overseas telegrams of an untold number of American citizens.

The N.S.A. is able to intrude on the communications of news agencies and newspapers, and communications of other governments, and conducts systematic intrusions on telephone communications in foreign countries, often picking up calls between American citizens, the sources said.

The N.S.A., possibly the most secretive of the agencies in what is termed the "intelligence community," is part of the Department of Defense and is charged with coordinating electronic intelligence gathering, along with the developing and breaking of codes.

There is a growing controversy within the intelligence community, several sources said, over whether the agency's activity is legal. Norman C. Boardman, chief of the agency's policy staff, declined to comment on the question on the ground that any comment might endanger national security.

But earlier this month, in hearings before the House Select Committee on Intelligence, an official of the agency testified that the N.S.A. believed all its activities were legal.

In the early nineteen-seventies, the agency's ability to monitor foreign cable traffic provided much of its assistance to a secret surveillance by the Central Intelligence Agency of American political dissidents, the sources said.

The N.S.A. monitored cable contacts between American antiwar groups and personalities and foreign governments and political groups, a source said, and provided material on former Attorney General Ramsey Clark, among others.

The N.S.A.'s contribution to the C.I.A.'s domestic surveillance program was mentioned cryptically in the recent report on the C.I.A. by the commission headed by Vice President Rockefeller.

The report said:

"Operation Chaos received materials from an international communications activity of another agency of the Government. The operation furnished a watch list of names to the other agency and received a total of approximately 1,100 pages of materials over all."

According to sources familiar with the N.S.A.'s operations, they are made possible by its "extraordinary" computer technology, which permits the sifting of millions of messages. Though there is no public total calculation of how many messages are transmitted in and out of the United States a year, in one communication category alone, transoceanic telegrams, 24,346,587 messages were transmitted in 1973.

This figure does not include messages sent over leased lines belonging to major companies and Telex Communications. When all three main communications methods are added together, one Government engineer said, "the N.S.A. would have to sift millions and millions of separate messages and billions of words."

The exact technology of the operation is a closely guarded secret, but several sources say it was effected by programing the computer to look for "trier words." The computer scans the message traffic and automatically selects for recording any message that contains the words it has been programed to watch for.

PICKS KEY WORDS

One source said that "the computer could be programed to record any message which contained the words oil, Saudi or Mideast and it would deliver messages with these subjects in them."

"Since businesses use cables far more than telephone for international communications, this kind of operation can tell you everything from their marketing plans to the intelligence their people are obtaining in a foreign country," he said.

The most valuable "product" from this program, one source said, is economic intelligence that enabled the United States Government to make international decisions on such matters as energy, grain sales to the Soviet Union and trade policies.

The law covering the disclosure of cable communications is more blurred than are the regulations covering wiretapping and bugging.

Section 605 of the Federal Code, covering telegraphs, telephones and radiotelegraphs, appears to prohibit the disclosure of material transmitted by international systems, but it is not precise on whether it covers the various modes of cable or written communications, nor is it precise on whether a Government agency has the right to contents.

BAR ON INTERCEPTION

Section 605 notes, "No persons not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, substance, purport, effect, or meaning of such intercepted communication by radio and use such communication (or any information therein contained) for his own benefit or the benefit of another not entitled thereto."

Though the statute uses the term "radio," it covers international communications, several Government experts agreed.

The legal questions would be materially affected if the carriers of international communications were covertly cooperating with the N.S.A. and "feeding" it the cable traffic, these experts said.

Relatively few companies are licensed to transmit international nontelephone messages. The main carriers are the International Telephone and Telegraph Corporation, the Radio Corporation of America and Western Union International. The bulk of cable traffic leaving this country is transmitted either through undersea cables or by communications satellites.

COOPERATION HELPFUL

Government engineers suggest that monitoring satellites is relatively easy, but that picking up material carried by undersea cables would be more easily accomplished with the carriers' cooperation. Many cables are jointly owned by the three main carriers.

According to recently published reports based on remarks by intelligence officials, the Soviet Union also intrudes on international transmissions and uses the material as an intelligence source.

One legislative aide who has done extended research on international communications and eavesdropping said that methods under development would make it possible for computers in the United States to

transmit files to computers in foreign countries over international satellite and cable connections.

"There simply is no law guarding this material from eavesdropping by government agencies, yet these transmissions may carry everything from credit files to doctors' reports on Americans," the aide said.

[From the Washington Star, June 18, 1975]

The New Party Line: Soviets Listen in on U.S. Long Distance Calls

(By James Deakin*)

With space satellites or antennae on top of the Soviet Embassy here, Russian technicians are believed to be monitoring thousands of long-distance telephone calls in the United States each year.

U.S. intelligence agencies are believed to be doing the same thing in Russia, especially in the field of military communications. But U.S. ability to listen in on Russian telephone traffic may be limited by the fact that the Soviet telephone system is less sophisticated.

In addition, a former State Department official charges that the National Security Agency is monitoring the overseas telephone calls and cables of many American citizens.

These and other aspects of U.S.-Soviet telephone surveillance were described this week after the Rockefeller Commission lifted the lid slightly on the secret world of electronic espionage in its report on the CIA.

The Senate committee headed by Sen. Frank Church, D-Idaho, plans to question officials of the CIA and the FBI about the Soviet monitoring, it was learned.

In its report on the CIA, the commission headed by Vice President Nelson A. Rockefeller stated that "Communist countries . . . appear to have developed electronic collection of intelligence to an extraordinary degree of technology and sophistication for use in the United States and elsewhere throughout the world . . ."

The commission said it believed that "these countries can monitor and record thousands of private telephone conversations."

Government sources said that these statements in the Rockefeller report referred to monitoring of long-distance telephone calls transmitted within the United States by so-called microwave relays.

Although the report referred to "Communist countries," in the plural, government sources made it clear that Russia was believed to be the only Communist nation with the ability to monitor such calls within the United States.

"Only a highly industrialized, computerized nation can do this," the sources said. They drew attention to what they said was a "concerted effort" by Russia to purchase American computer technology "and an equally concerted effort by the U.S. to prevent them from buying it."

As described by government officials, the monitoring of long-distance calls consists of picking up the calls as they are transmitted

---

*James Deakin is a correspondent of the St. Louis Post-Dispatch.

between microwave stations. In the United States, these stations are about 20 to 25 miles apart.

About 70 percent of the long-distance calls in the United States are transmitted by microwave relays, a spokesman for the American Telephone and Telegraph Co. said. The remainder are transmitted by underground cables or old-fashioned telephone wires on poles.

To pick up calls between microwave stations, the intercepting antenna must be in the "line of sight" between the stations, government sources said. Microwave signals can be transmitted only in a "line of sight," meaning that there are no obstructions such as mills or tall buildings in the way.

Government sources said Russian agents could intercept long-distance cable calls with a high antenna on the roof of the Soviet embassy here. Computers then would separate out the bundles of calls in each microwave relay.

"Why do you think the Russians are so anxious to build their new embassy on the Mt. Alto site?" a government source said. "It is a much higher elevation than the site of the present embassy and would give them a much better line of sight for intercepting microwave relays."

The Soviet government has been negotiating for several years to build a new embassy on the site of the old Mt. Alto Veterans Hospital on Wisconsin Avenue. This is one of the highest elevations in the District.

The roof of the present Soviet Embassy, on 16th Street, is festooned with aerials. This has led U.S. intelligence agencies to conclude that the embassy has the ability to monitor many types of communications within this country, John D. Marks, a former State Department intelligence officer, said.

Marks, however, believes that a high antenna on the roof of the Soviet embassy would have only a limited capacity to intercept microwave-relayed long-distance calls and that Russia more likely is using one or more fixed space satellites to do most of its monitoring.

"If you just visualize the line of sight from one microwave tower to another, at some point it goes into outer space," Marks said. "You just put your satellite there, in a fixed position, and pick up the relays."

Because most local telephone calls within a city or a metropolitan area are transmitted by underground cables or telephone wires on poles, it is believed that most of the Russian monitoring involves long-distance calls.

The Russian civilian telephone system does not use microwave relays to the extent that the U.S. system does, government sources said. As a result, they said, the U.S. intelligence agencies may not be able to intercept Russian long-distance calls to the same extent.

"But I can give you a categorical assurance that we are reading Soviet microwave communications, especially military communications," Marks said. "But we are not necessarily doing this from the U.S. Embassy in Moscow."

Not only is the United States doing the same thing with Russian microwave relays, but "I have personal knowledge from my own State Department career that the National Security Agency has been

monitoring overseas telephone calls and cables by American citizens," Marks said.

Marks drew attention to a paragraph in the Rockefeller Commission report that said that the CIA had "received materials from an international communications activity of another agency of the government," as part of "Operation Chaos."

Operation Chaos was a secret CIA investigative and surveillance program that tried unsuccessfully to prove that anti-war and civil rights groups in the United States were being directed and financed by foreign elements.

The Rockefeller report said that the CIA, as part of Operation Chaos, "furnished a watch list of names to the other agency and received a total of approximately 1,100 pages of materials . . ."

Marks identified the other agency as the NSA. The material apparently consisted of transcripts of overseas telephone calls, cables and other communications by U.S. citizens.

"The materials concerned for the most part antiwar activities, travel to international peace conferences and movements of members of various dissident groups," the Rockefeller report said.

Although the report said that the furnishing of material to the CIA stopped when Operation Chaos was terminated in March 1974, Marks pointed out that the report did not say that the surveillance of overseas communications by the NSA had stopped.

Government sources said that the section of the Rockefeller report dealing with Soviet monitoring of calls in the United States was written by Rockefeller himself. They said the vice president wanted the material included in the report, apparently as a justification for similar CIA activities.

"There was some intense feeling within the commission that it (the material on Russian monitoring) had no place in the report, because it was felt that the commission's mandate was to look into the CIA and not into the KGB (the Soviet Intelligence Agency)," the sources said.

They said Rockefeller's view prevailed, although the section was shortened because of opposition from other members or staff personnel of the commission.

[From the Washington Post, Dec. 5, 1973]

U.S. Tapped Top Russians' Car Phones

(By Laurence Stern)

The U.S. government systematically monitored the limousine radios of top Soviet officials in Moscow for several years ending in 1971, according to former intelligence sources familiar with the operation.

The project, code-named Gamma Gupy, was terminated in late 1971 after some details of its operation were disclosed by columinst Jack Anderson.

A former intelligence official who had access to the transcripts of the monitored conversations in Moscow described the system as one of

the most valuable intelligence pipelines the United States had in the Soviet Union.

Among the Soviet officials who were tapped by the Gamma Gupy system were Soviet Party General Secretary Leonid Brezhnev, President Nikolai Podgorny and Premier Alexi Kosygin.

The top-secret operation was conducted by the Central Intelligence Agency in collaboration with the National Security Agency—the government's chief gatherer of intelligence by electronic means.

A former intelligence official who monitored the Gamma Gupy interception traffic said that the conversations revealed few major strategic secrets but "gave us extremely valuable information on the personalities and health of top Soviet leaders. But we didn't find out about, say, the invasion of Czechoslovakia. It was very gossipy—Brezhnev's health and maybe Podgorny's sex life."

The CIA had built a facility a few miles from its Langley, Va., headquarters, where incoming traffic from the super-secret Moscow tap was monitored, according to knowledgeable sources.

Anderson's column, which appeared on Sept. 16, 1971, did not specify the means by which the conversations of top Kremlin officials was transmitted to Washington.

Intelligence sources here said the Soviet limousine telephone traffic was susceptible to interception because the phones were not sufficiently "scrambled"—a technique for making spoken words snoop-proof.

(The name of the telephone tap operation is reportedly an NSA code classification indicating the priority and secrecy of the mission.)

Anderson said yesterday that after his column appeared he was invited to lunch with then CIA Director Richard M. Helms and asked by Helms not to divulge the means by which the interception was made. Helms also requested, Anderson said, that the project not be referred to again.

The columnist said his original source on the Soviet tap told him the Russians had already realized their phone traffic was being monitored. Otherwise, he insisted, he would not have written the column. Anderson said he agreed not to mention details of the system and specifically promised Helms not to allude to the operation in his book, The Anderson Papers.

A CIA spokesman said yesterday the CIA had no comment on any aspect of the matter.

There was only one other published reference to the Moscow taps—a passing allusion in The Wall Street Journal of May 8, 1973 to the fact that "the CIA was busily monitoring the radiotelephones in Mr. Brezhnev's limousine as he sped around Moscow and out to the country for weekends."

A former intelligence official who had access to the Gamma Gupy traffic characterized the original 1971 leak as "completely gratuitous—it served no purpose and blew our best intelligence source in the Soviet Union."

There has been widespread conjecture that the White House Special Investigations Unit, known as the Plumbers, was investigating a news leak in the fall of 1971 that compromised an important intelligence source in the Soviet Union.

White House special counsel J. Fred Buzhardt had been seeking to discourage the indictment of John D. Ehrlichman, Charles W. Colson

and Egil (Bud) Krogh, all former presidential aides, on grounds that the prosecution of their cases would jeopardize national security.

Erhlichman, testifying last June in his California trial, said the responsibilities assigned the Plumbers included the Pentagon Papers, the SALT talk leak "and . . . the third one which had to do with the disclosure of a CIA source in a foreign country—and then the fourth one, which I am not at liberty to discuss."

The nature of the third and fourth news leaks has never been officially identified.

[From the Washington Post, Dec. 9, 1973]

U.S. Spy Unit Ultra-Secret

EVEN ITS NAME MENTIONED ONLY ACCIDENTALLY

(By Laurence Stern)

In the arcane and heavily classified world of "overhead" reconnaissance and spy satellite intelligence, the existence of the National Reconnaissance Office has been one of the best kept trade top secrets.

The name of the organization, in fact, is top secret, and, according to intelligence officials, has appeared in public print only once before—by inadvertence.

Yet the NRO, which is funded primarily through Air Force appropriations, spends an estimated $1.5 billion a year acquiring and managing the most sophisticated, elusive and expensive force of spies that has ever been recruited into the government's service.

Its customers include the Central Intelligence Agency, National Security Agency, Defense Intelligence Agency and the White House. Its operatives bear such names as SR–71, Samos, Agena, and "the Big Bird." Its activities are screened off from all but a relative handful of specialists in the national security bureaucracy who carry some of the highest and most specialized clearances issued by the government.

Curiously enough, the only reference to NRO that has been made in a public government document was last Oct. 12 in a report of the Special Senate Committee to Study Questions Related to Secret and Confidential Government Documents. The drafters of the report unwittingly breached security by listing, along with CIA, DIA and NSA on the concluding page, the National Reconnaissance Office.

And, more obliquely, Sen. William Proxmire (D-Wis.) alluded to the NRO's mission in a recent statement challenging the appointment of Lockheed Aircraft Corp. reconnaissance satellite expert James W. Plummer as under secretary of the Air Force.

In questioning Plummer's nomination on conflict-of-interest grounds, Proxmire made a pointed observation:

"Normally, the under secretary of the Air Force has jurisdiction over certain intelligence matters and sits on a special committee that directs manned and unmanned overhead reconnaissance, including spy satellite programs. These critical projects have run into the billions of dollars—money that flows to defense contractors such as Lockheed."

Plummer has been with Lockheed since 1955. The California-based firm is the principal corporate contractor in the so-called "black" reconnaissance satellite programs carried out by NRO.

From the "skunk works," as specialists describe the facility, of Lockheed spy plane developer Kelley Johnson in Nevada also emerged the U–2 and SR–71. "The U–2 was perhaps the only government spy project to have a cost under-run and to exceed the promised performance standards," said one expert on the program. Lockheed was also the prime contractor on the C–5A, which was plagued by $2 billion in combined cost overruns.

In addition to the conflict-of-interest issue in Plummer's appointment, congressional investigators are looking into the possibilities of overruns in the supersecret reconnaissance satellite programs under NRO's jurisdiction.

"I've never heard of one of these programs that didn't have enormous cost overruns," said one Defense Department official who has worked first-hand with some of the spy satellite operations. The opportunities for breaking cost and performance commitments are greater in spy satellite programs, this official said, because of the atmosphere of secrecy and narrow channels of accountability in which they operate.

NRO's existence is shielded from senior congressional intelligence overseers. Former high-ranking staff members of the National Security Council, who were cleared for some of the most sensitive intelligence material to reach the President's desk, acknowledged in interviews that they had not been informed about it.

"This is a black program and you're not supposed to know it exists," said one Pentagon administrator. For the past several years its supervision has nominally been in the hands of the Under Secretary of the Air Force. Operations and procurement have been handled through the office of the Secretary of the Air Force, according to Defense Department sources.

Its intelligence projects, labeled ELINT (for electronic intelligence) and COMINT (for communications intelligence) are parceled out under special code names to the government "consumers"—such as CIA or NSA. The users may get the product of the secret reconnaissance, such as monitoring of Chinese nuclear tests, or radio transmissions in the Soviet Union, without being told of the collection techniques. This is known as "compartmentalizing" of intelligence data.

Since the inception of the U.S. reconnaissance satellite program in the mid-1950s to 1970 some $10 to $12 billion had been spent on the spy birds, according to an estimate by aviation and space writer Philip J. Klass in his book, "Secret Sentries in Space." Since then the outlay may have grown by about $5 billion.

Overhead reconnaissance has proven of enormous value in providing more realistic assessments of such things as Soviet ballistic missile capability, both offensive and defensive. It helped, in fact, to defuse public anxieties over the missile gap in the early 1960s. The most publicized use of the program was to support President Kennedy's contention that the Soviet Union was installing offensive missiles in Cuba.

But congressional investigators in yet unpublicized inquiries are raising questions about relationships between corporate contractors and the super-secret programs being carried out under the aegis of NRO and other military intelligence agencies.

Proxmire's concern about the Plummer appointment is one example of this. Air Force Secretary John L. McLucas came to the government from the Air Force think tank, MITRE. Assistant Air Force Secretary for procurement Frank Schrantz comes from Boeing.

"There has been a tendency, stronger than ever in recent months, to put executives of contractor agencies in these key positions," said one veteran Defense Department official. "Not that there is anything personally wrong with these men. But all their attitudes have been shaped by their experience working for contractors."

The late Allen Ellender (D-La.), former chairman of the Senate Appropriations Committee, was one of the few members of Congress privy to some of government's best-kept intelligence secrets, and rhubarbs.

"If you knew how much money we spend and how much money we waste in this area," Ellender said in a 1971 interview, "it would knock you off of your chair. It's criminal."

Whatever that amount might be will probably never appear in the public domain.

[From the New York Times, Feb. 26, 1976]

House Panel Calls for Five Contempt Citations in Inquiry on U.S. Surveillance

(By Robert M. Smith)

Washington, Feb. 25.—A House subcommittee voted today to recommend contempt citations against three special agents of the Federal Bureau of Investigation, a former F.B.I. agent and an employee of the National Security Agency because they refused to provide information about the Government's interception of telegraph and Telex messages.

The Government Information and Individual Rights subcommittee recommended the citation, by a vote of six to one, after the witnesses had refused to provide information on the ground that they had been instructed by their superiors—Attorney General Edward H. Levi and Deputy Secretary of Defense William P. Clements, Jr.—not to produce documents or testify.

Mr. Levi and Mr. Clements acted in response to a memo from President Ford in which, they said, the President invoked executive privilege.

Mr. Ford's memo explained that after reviewing subpoenas issued by the subcommittee, the President had "concluded that the scope of the records sought is so extremely broad as to encompass records containing the most sensitive national security information, and the public interest requires that the records not be disclosed to the committee."

PLANS FOR LEGISLATION

Mr. Ford's memo came one day before he sent to Congress, last Wednesday, a message in which he said, "I will meet with appropriate

leaders of Congress to try to develop sound legislation to deal with a critical problem involving personal privacy—electronic surveillance."

At today's hearing, four of the witnesses refused to produce documents that had been subpoenaed as well as to answer questions. One witness, Joseph J. Tomba of the National Security Agency—possibly the most secretive of the organizations that make up the nation's "intelligence community"—maintained that he had no documents "in my control, under my dominion to produce."

When pressed by Representative Toby Moffett, Democrat of Connecticut, as to whether he meant he did not have the authority to produce the documents but would otherwise be able to, Mr. Tomba said that he would not answer the question "based on instructions from the Deputy Secretary of Defense."

President Nixon invoked executive privilege on numerous occasions and thereby strained his relations with Congress. Some of Mr. Nixon's predecessors also invoked the privilege. The doctrine holds that Presidential communications within the executive branch are protected if disclosure would hamper the orderly functioning of government.

The most notable instance in which President Nixon used the doctrine was in resisting a prosecution subpoena for tapes and records of 64 White House conversations. The Supreme Court rejected Mr. Nixon's contention that he had an absolute executive privilege but gave constitutional stature to executive privilege for confidential communications.

The Court said that claims of executive privilege should be given great weight—because of the importance of confidentiality to the proper functioning of the Presidency—but added that claims of privilege would sometime have to fall in the face of competing needs for the material being sought.

Representative John E. Moss, Democrat of California, warned one witness today that he would have to answer the questions he was putting or be summoned before the Subcommittee on Oversight and Investigation, which Mr. Moss heads.

Mr. Moss also said that "the real contempt here has been committed by the Attorney General of the United States and the President of the United States."

When Joe R. Craig, a former F.B.I. agent and the first witness said, "by letter dated Feb. 23, the Attorney General of the United States has instructed me not to testify in response to this subpoena," Mr. Moss declared loudly:

ACTIONS LAID TO TWO

"The Attorney General is without any authority. It is the most outrageous assumption, the most arrogant display by the Attorney General I have ever seen. Some damn two-bit appointee of the President is not the law-making body of this country."

The witnesses were pressed as to whether they had a constitutional basis for refusing to produce the documents or answer the questions. They generally responded by saying they were relying solely on the instructions of the Attorney General or the Deputy Secretary of Defense.

Mr. Moss told Mr. Craig that the Attorney General's letter to him did not constitute a basis for refusing to answer. He added "It's not

the Attorney General's liability, it's your personal liability" for not answering.

All the witnesses except Mr. Craig had a Justice Department lawyer with them.

In light of the personal liability they might incur, Mr. Moss suggested that the witnesses should have "private counsel interested in their welfare, not in their being sacrificial lambs" for the Justice Department.

Representative Bella S. Abzug, the Manhattan Democrat who heads the subcommittee, said that in private meetings Attorney General Levi had warned her that national security might be impaired by the testimony she sought but she said that he had refused to specify how.

She also said that she could not understand "the assertion of executive privilege by a private corporation," Western Union International. In a letter to her lawyers, the company cited "the order of the President, signed by Attorney General that Western Union International not produce any documents responsive to such subpoena."

In addition to Mr. Craig and Mr. Tomba, the subcommittee recommended contempt citations against John P. Loomis, Walter C. Zink and David G. Jenkins, all F.B.I. agents.

[From the New York Times, April 3, 1976]

Tapping Computers

(By David Kahn*)

Great Neck, N.Y.—Like people, computers talking to one another can be wiretapped. To protect themselves, more and more companies, such as the oil giants and banks, are putting their digital correspondence into secret form.

This has led to a demand for a common cipher—a system that would both permit intercommunication among computers and safeguard the privacy of data transmissions. The National Bureau of Standards, with the help of the National Security Agency, the Government code-making and code-breaking body, has proposed one.

The interesting thing is that while this cipher has been made just strong enough to withstand commercial attempts to break it, it has been left just weak enough to yield to Government cryptanalysis.

Under the plan, all participating computers would incorporate the cipher hardware—tiny integrated-circuit chips, each mounted on an inch-long plastic wafer. For privacy, each pair of correspondents would have an individual key—a string of zeroes and ones, each string different.

The sender would use this to put outgoing messages into cipher; the recipient, to decipher incoming texts. Competitors would not be able to use their keys to unlock these messages any more than your neighbor's house key will open your front door. And even if a competitor has somehow gotten hold of an original message, so many keys are to exist as to make it impractical for him to find the right one and so uncover other messages enciphered in it.

*David Kahn, a journalist, is author of "The Codebreakers."

Each individual key in the cipher as proposed would have 56 zeroes and ones, or bits (short for "binary digits"). This length, two computer scientists at Stanford University say has been craftily chosen to make it too expensive for private firms to cryptanalyze the digital messages—but not for the Federal Government.

Prof. Martin E. Hellman and a graduate student, Whitfield Diffie, suppose that someone wanted to crack these messages by "brute force"—that is, by trying all keys possible for a particular situation. This someone could build a computer using a million of the chips. It could test a trillion keys per second. With 56 bits, the total number of possible keys is 70 quadrillion. The computer could thus exhaust all keys in 70,000 seconds, or less than 20 hours.

In large quantities, Hellman and Diffie say, the chips would cost perhaps $10 each at today's prices. To design and build a million-chip machine would come to about $20 million. If this were amortized over five years, the cost of each day's operation—in effect, the cost of each solution—would amount to about $10,000.

Who, they ask, has the money to spend on such a machine and the need for daily solutions that would justify it? Only the Government. For private industry, the gains would hardly be worth the investment.

Now suppose the key length were 48 bits. The price of a machine to generate a solution a day would fall to $78,000 and the cost of each solution to $39. On the other hand, if the length were 64 bits, the price of such a machine would soar to $5 billion and of each solution to $2.5 million. This seems beyond even the bottomless pocketbooks of the intelligence agencies.

The National Security Agency and National Bureau of Standards argue that the two men's assumptions are off and that people wanting this information would find cheaper ways to get it than by breaking codes. But just because a house has windows is no reason for not locking the front door, Hellman and Diffie reply, and computer security experts at International Business Machines, at Bell Telephone Laboratories, at Sperry Univac, and at the Massachusetts Institute of Technology agree with them that 56 bits is too small. Indeed, one major New York bank has decided not to use the proposed cipher, called the "data encryption standard," in part for the same reason. And the House of Representatives Government Information and Individual Rights Subcommittee is now looking into the matter.

Hellman and Diffie urge a key length variable at the will of the user up to 768 bits, which they claim can be done at a negligible increase in cost. This would render messages insoluble forever, despite the continuing drop in computation costs.

Why should the National Security Agency be so passionately interested in the 56-bit key that it asked to attend a meeting that Hellman set up on the question and flew a man across the country for it? The N.S.A. expert declined to say. But one obvious reason is that, with a solvable cipher, N.S.A. would be able to read the increasing volumes of data that are flowing into the United States time-sharing and other computer networks from abroad.

The problem is that it would gain this information at the expense of American privacy. For it would also be able to crack domestic computer conversations as well as masses of enciphered personal files. And recent history has shown how often an agency exercises a power simply because it has it.

But perhaps the intelligence is worth it? The answer to that was given a long time ago. "For what shall it profit a man if he shall gain the whole world and lose his own soul?"

[From the Washington Star, May 12, 1976]

In Focus—Spy Satellites Getting Priority in Soviet Space Program

ENGLISH AMATEUR KEEPS THE FREE WORLD INFORMED

Moscow, 5 May (Tass).—The artificial earth satellite Cosmos 817 was launched in the USSR today. It was launched with the following parameters: initial period of rotation, 89.5 minutes; maximum distance from the earth, 347 kilometers; minimum distance, 178 kilometers; inclination of orbit, 65 degrees. The apparatus is functioning normally.

(By Henry S. Bradsher)

In the week since the official Soviet news agency distributed that brief announcement on authorization of the Strategic Rocket Forces, Cosmos 817 has been orbiting the earth while its apparatus functions normally on an important—but carefully unspecified—assignment.

It is photographing areas of interest to the Soviet armed forces. The 817th launching in a series of earth satellites that was originally asserted to be for scientific research is a "spy in the sky" reconnaissance vehicle.

Sometime between Monday and next Wednesday it will probably be brought back to earth and recovered in the Kazakh region of Soviet Central Asia. The main Soviet space center, known as the Baykonur Cosmodrome, is located in the desert region near a little railroad stop named Tyuratam.

The nature of Cosmos 817 and its probable landing time can be deducted on the basis of observations in the United States and England on the secret Soviet space program. The height of the orbit—between 110 and 215 miles, for those who have not yet been forced to adjust to the metric system—and its angle of inclination with the equator disclose that it is one in a series of what Western experts call the "military observation recoverable satellites," which usually stay up 12 to 14 days.

When the first Cosmos satellite was launched on March 16, 1962, to open a new Soviet launch site at Kapustin Yar on the lower Volga River, it had the scientific research purpose claimed for it. So did the next two, but the fourth just six weeks later on April 26 began Soviet space reconnaissance programs.

Now spy satellites are the largest single element in a space launching program that is three times as active as the American one. But within the program are numerous other functions ranging from watching the U.S. Navy around the world to relaying communications across the vast span from Moscow to the Soviet Far East.

Last year, 34 out of 139 payloads which the Soviet Union put into space with 89 launchings—some rockets lofted as many as eight satel-

lites by the same techniques as multiple warheads on intercontinental ballistic missiles—were reconnaissance satellites.

According to calculations of Dr. Charles S. Sheldon II of the Library of Congress, this raised total Soviet spy satellites since 1962 to 328, more than a quarter of the 1,177 space payloads since the first Sputnik was launched in 1957.

Sheldon is the Chief of the Congressional Research Service's science policy research division. Working from public material—indeed, deliberately shunning secret military information in order not to inhibit his deductions from unclassified sources—he has become the leading Western source of interpretation on the basic data about Soviet space activities.

His count shows 182 communications satellites through the end of 1975, 42 electronic ferreting, 12 naval monitoring and a lot of other miscellaneous military purposes. Various scientific purposes account for some 150 payloads, and the Soviet version of the weather satellite which produces pictures for television weather reports numbers 38.

The program has also lumped in the Soviet manned space flights, shots at the moon and explorations of other planets. The Soviet Union has been particularly active in probing the incredibly dense, hot atmosphere of Venus.

How much this has cost the Soviet Union in cash and in resources and talent diverted from ordinary earthbound needs is never discussed publicly by Kremlin leaders. But one of the Soviet versions of American astronauts, who are called cosmonauts, Gen. Alexei Leonov, said last month that every ruble spent on space research has already been returned many times over to the national economy.

Leonov did not give specific details in the TASS account of his remarks for the 15th anniversary of the first manned space flight. It was made April 12, 1961, by Cosmonaut Yuri Gagarin, who was later killed in a training plane crash.

American specialists say, however, that the Soviet space program has had little fallout for civilian benefit. The U.S. space program has given a whole series of new devices to the American public, such as new types of fasteners that replace zippers. But the muscle bound Soviet economy is not organized to spread into public consumption those inventions made within the secrecy of a military-run program.

Space activities have a long history in Russia. Konstantin Tsiolkovsky is claimed by the Soviets, with more validity than many other Soviet claims of inventive firsts, to have been the father of world rocketry. But it was not until the Red Army captured a lot of Nazi German scientists and equipment in 1945 that the space program really got underway.

By 1957 a top-priority effort had produced the SS6 intercontinental ballistic missile, which startled the world by hurling the first satellite into orbit. With upper stages added for more thrust, it is still the mainstay of the Soviet space program.

Some foreign experts have looked upon the SS6 as a Model T launch vehicle, crude compared with those now used by the United States and such other space activists as the French and Japanese. The crudity of the whole Soviet program was clearly seen last year in the manned

space link-up between the highly sophisticated American capsule and a rough-but-ready Soviet device.

But it works. The Soviet Union was the first into space. The United States rushed to catch up. From 1958 to 1966 this country sent up more earth satellites and vehicles to the moon or the planets, and since then it has set most of the records for men in space. But beginning in 1967 the Soviets have been more active, maintaining the 3:1 ratio of launches for the last three years.

In many ways the two programs are comparable. Both superpowers have their spy satellites, for instance. These are officially recognized in two 1972 Soviet-American agreements.

They provide that "each party shall use national technical means of verification at is disposal" to monitor compliance with the treaty against anti-ballistic missiles and the interim agreement on limiting strategic weapons. The means are reconnaissance satellites, and each side "undertakes not to interfere" with the others.

Both countries have, however, tested the use of missiles to shoot down enemy objects in space. The Soviets made seven tests over several years beginning in 1968, causing concern for American reconnaissance, communications and navigation aid satellites, but halted the program in 1971.

Then Cosmos 803 was sent up last Feb. 12 and on Feb. 16 Cosmos 804 was launched. The first appeared to have been a quarry, the second a hunter, thus renewing testing of devices that can maneuver alongside a satellite, inspect it through sensing devices and then destroy it with an explosion of debris.

Perhaps significantly, the new test came just a few months after China had for the first time lofted a satellite and recovered it. Peking is apparently working toward an ability to watch Soviet troops on its borders.

Some Pentagon sources think the Soviet Union now has destroyer rockets poised to knock down American spy satellites, but other observers are not so sure. The United States has had destroyer rockets on Johnston and Kwajalein islands in the Pacific, where it tested anti-ballistic missile systems.

The superpowers' spy satellite programs have many similarities. Leaks in Washington have told of special U.S. reconnaissance devices being put up to watch flashpoints during international crises, such as the October 1973 Middle East war. The Soviets have done the same.

The Soviet Strategic Rocket Forces have made special launchings and have maneuvered satellites into different orbits in order to focus on crisis spots. The last Middle East war, the 1971 Bangladesh war toward which the United States sent an aircraft carrier task force, and French nuclear weapons tests in the South Pacific have all attracted particular Soviet attention.

This focusing of activity presumably has been noticed by American military specialists, but public knowledge has come from Geoffrey E. Perry of the Kettering Grammar School in England. A space buff like Sheldon, Perry has made his own radio intercepts and used information collected by U.S. and British government agencies to arrive by deduction at basic insights into Soviet space activities.

79-064—76——72

The agencies include the North American Air Defense Command. It keeps track by radar of the thousands of bits of junk now floating around in space in order to be able to tell when some potentially threatening new missile or satellite goes up. The National Aeronautics and Space Administration's Goddard Space Flight Center also compiles data on Soviet activities.

Satellite communications have been important for the Soviet Union. Starting in 1965 a Molniya series was used to allow people in Vladivostok to see Moscow's Red Square parades live.

The Molniya satellites are blasted into a highly eccentric orbit. The first one swooped to within 340 miles of the Southern Hemisphere and then soared 24,775 miles above the Northern Hemisphere, while others have been higher. This enabled them to have line of sight communications with the Soviet Union for some nine hours apiece and out of sight only briefly.

Two years ago the Soviets began using synchronized orbits of Raduga satellites "parked" over points on the equator. The United States had long found this the most effective orbit for communications but the Soviet Union's northerly position made it more difficult.

Communications satellites now talk to ground stations, which amplify their weak signals and rebroadcast them to final destinations, whether military units or home television receivers. But within technical sight is the prospect of satellites' beaming programs directly into homes.

This erosion of its control over domestic information media worries the Kremlin. It does not want American television programs going directly to the Soviet people. It has therefore been arguing in the United Nations to try to get a ban on direct broadcasting from space.

The emphasis seems to have faded out of the Soviet manned space program almost as completely as it has from the U.S. program after completion of the moon trips.

But the United States is working on a space shuttle to make the use of orbital platforms both easier and more economical, and an East German report indicates the Soviets are also trying to develop reusable spacecraft to replace the present system of throw-away rockets. These could open up a new generation of men in space carrying out both scientific and military tasks.

Soviet space probers have for a decade missed few "windows" when the alignment of planets was advantageous for the launching of rockets to Mars and Venus. But the success rate has been low.

Sometimes rockets have failed to break out of earth orbit, and these failures have been hidden by listing them as Cosmos satellites. Other probes have gotten to their targets but failed to return the expected data because their crudity has not given them adequate operational ruggedness.

It was the Russians who got the first photos of the far side of the moon, but it was the United States that provided the overwhelming bulk of the earth's present knowledge of its natural satellite.

[From the New York Times Magazine, May 16, 1976]

Big Ear or Big Brother?

THE NATIONAL SECURITY AGENCY WAS CREATED 23 YEARS AGO TO INTERCEPT AND DECODE THE MESSAGES OF FOREIGN GOVERNMENTS WHO SAID IT SHOULD LISTEN IN ON AMERICANS AT HOME?

(By David Kahn*)

Room 6510 at the State Department is a warren of windowless offices with a special cipher lock on the door. Scrambler teletypewriters, shielded by special walls so that none of their radiation can escape, tick out a stream of material. Another door bars an inner area to all but perhaps 5 percent of the officials at State. This is the LDX room—long-distance Xerox. Here, the scourings of the globe's electronic environment flood in.

The environment is heavy with traffic—the *didahdidah* of Soviet Army radiograms in code or in clear; the buzzings of foreign air-defense radars; the whines of high-speed radio-teletypewriter circuits carrying diplomatic dispatches; the bleeps of missile telemetry; the hums of the computer-data links of multinational corporations; the plain language of ordinary radio messages; the chiming sing-song of scrambled speech. Moving on these varied channels may be Soviet orders to transfer a regiment from one post to another; Chinese Air Force pilots complaining during a practice flight about deficiencies in their equipment; Saudi Arabian diplomats reporting home from a meeting of OPEC. Tens of thousands of such messages are intercepted daily around the world and beamed to a complex at Fort Meade, Md., for decoding and relaying to the State Department and, simultaneously, to the White House, the Defense Department and the C.I.A.

The tall, bespectacled Air Force general sat down behind a table in the high, colonnaded Caucus Room of the Old Senate Office Building. Television focused its dazzling lights upon him and recorded his gestures. Two business-suited aides pulled up their chairs on either side of him. Before him sat the members of the Senate's Select Committee on Intelligence. A gavel banged, and the hearing began.

In appearance, the event resembled the start of thousands of Congressional hearings. What distinguished this one, last Oct. 29, was that, for the first time, the head of the largest and most secretive of all American intelligence organs had emerged from obscurity to describe some of his agency's work and respond to charges that it had invaded Americans' privacy. The big officer was Lieut. Gen. Lew Allen Jr., current director of the National Security Agency. N.S.A. is America's phantom ear. And sometimes it has eavesdropped on the wrong things.

In addition to sucking up and disgorging its daily load of intercepts from abroad, the N.S.A. had improperly eavesdropped on the conversations of many Americans, such as the antiwar protesters Benjamin Spock and Jane Fonda and the Rev. Ralph Abernathy, successor to Dr. Martin Luther King Jr., current director of the National Bureau of Narcotics and Dangerous Drugs and other Government agencies,

*David Kahn, assistant professor of journalism at New York University, is the author of "The Codebreakers."

its vast technological capabilities had invaded the domestic field, which they were never intended to do. The committee wanted to know about an N.S.A. activity dubbed the "watch list."

General Allen testified that, in the early 60's, domestic law-enforcement agencies asked the N.S.A. for information on American citizens traveling to Cuba. The assignment, he said, was reviewed by "competent external authority"—two Attorneys General and a Secretary of Defense. All approved it, and the idea of using the N.S.A. for such purposes spread rapidly through the Government. The drug bureau submitted the names of 450 Americans and 3,000 foreigners whose communications it wanted the N.S.A. to watch. The F.B.I. put in a list of more than 1,000 American and 1,700 foreign individuals and groups. The Central Intelligence Agency, the Defense Department and the Secret Service also submitted watch lists. Altogether, General Allen said, some 1,650 American names were on the lists, and the N.S.A. issued about 3,900 reports on them.

But all this is over, he said; he personally abolished the "watch list" when he took over the agency in 1973.

The general's assurance did little to overcome the committee's overall concern—and that of many other Americans. For both prior to and since that hearing, disclosures in Congress and elsewhere have indicated a multifaceted practice of using the N.S.A. in ways that threaten American freedoms. For instance:

☐ The N.S.A. persuaded three major cable companies to turn over to it much of their traffic overseas. It was partly through this operation, code-named Shamrock, that the N.S.A. complied with the "watch list" assignment. At one office, the N.S.A. man would show up between 5 A.M. and 6 A.M., pick up the foreign messages sorted out for him by company employees (who were said to have been paid $50 a week for their cooperation), microfilm them and hand them back. When messages began to move on tape, the N.S.A. got them in that form. The agency took some 150,000 messages a month, 90 percent of them in New York, and thousands of these were distributed to other Government bodies. Congress got wind of Shamrock, however, and a year ago, after 28 years and millions of private telegrams, Secretary of Defense James R. Schlesinger had to terminate the operation.

☐ A previous N.S.A. director co-signed the notorious plan of White House aide Tom C. Huston, to penetrate organizations considered security threats by the Nixon Administration. The agency furnished Huston with several suggestions; one of them seems to have been to let the N.S.A. eavesdrop on domestic American communications. Huston conceded that the plan would use "clearly illegal" techniques. But the N.S.A. has acknowledged that it "didn't consider . . . at the time" whether its proposal was legal or not. The Huston plan was never implemented, but, said the Senate Watergate Committee, the "memorandum indicates that the N.S.A., D.I.A. [Defense Intelligence Agency], C.I.A. and the military services basically supported the Huston recommendations."

☐ Former President Nixon acknowledged in a recent deposition to the Senate Intelligence Committee that he had used the N.S.A. to intercept American nonvoice communications. He said he wanted to discover the source of leaks from the staffs of the National Security Council and the Joint Chiefs of Staff.

☐ The agency is said to have passed reports on what prominent Americans were doing and saying abroad directly to Presidents Johnson and Nixon. Once, for example, the agency informed Johnson that a group of Texas businessmen involved in private negotiations in the Middle East had claimed a close relationship with him to improve their bargaining position.

☐ Two Stanford University computer scientists have recently accused the N.S.A. of promoting its own interests at the expense of the public's in a standard cipher proposed by the Government for computer networks. At issue is the key that would afford secrecy between pairs of users. The scientists accuse the N.S.A. of maneuvering to get industry to accept a key that, while too complex for rival businesses to try to solve, would be susceptible of cracking by the N.S.A.'s superior capabilities. That would permit the agency to raid the economic data flowing into the computer network, and to penetrate personal-data files enciphered for security.

☐ In the whole area of economic intelligence, N.S.A. interception has been developing rapidly. The House Intelligence Committee, in its report, expressed concern over the resultant "intrusion . . . into the privacy of international communications of U.S. citizens and organizations."

At the root of General Allen's appearance before the Senate Intelligence Committee, and of the entire Congressional investigation of the N.S.A., lay the question: Who authorized these abuses? What was there about the agency's legal basis that permitted it to invade privacy at the request of other Government agencies—and with so little qualm? Was the final authority the President's—and, in that case, was he not armed with powers to play Big Brother beyond the worst imaginings of the recent past?

"[The N.S.A.'s] capability to monitor anything . . . could be turned around on the American people," said the committee's chairman, Senator Frank Church. "And no American would have any privacy left. There would be no place to hide. If a dictator ever took charge in this country, the technological capability that the intelligence community has given the Government could enable it to impose total tyranny."

How essential to the nation's security is the National Security Agency? How can a balance be struck between the legitimate needs it serves and the freedoms it has shown itself capable of undermining? How did the whole problem originate?

Signals intelligence reaches back in America to the founding days of the Republic. But it matured only in World War I, with the widespread use of radio. During World War II, it became the nation's most important means of gathering secret information. When the Iron Curtain clanged down, the United States wanted to preserve these extraordinary capabilities. In 1952, President Truman issued a directive transforming the Armed Forces Security Agency, the interservice arm for signal intelligence, into the National Security Agency, serving all branches of government.

Therein lay the first pitfall. Unlike the C.I.A., in which all intelligence functions were centralized in 1947, the N.S.A. was not formed by act of Congress, with a legislative charter defining the limits of its mission. The cryptologic empire has only a Presidential directive

as its legal base. So shadowy has been the N.S.A.'s existence, however, that the text of the seven-page directive has never been made public.

This obsession with secrecy is well reflected by the agency's headquarters. At the edge of Fort Meade, just off the Washington-Baltimore Parkway, it is ringed by a double chain-link fence topped by barbed wire with six strands of electrified wire between them. Marines guard the four gates. Inside lie a modern, three-story, square-A-shaped structure and, within its arms, a boxy nine-story building. From the latter, in particular, emanates a chill impersonality, quite different from the flashiness of C.I.A. headquarters in McLean, Va. Topped by a frieze of antennas, the only sign of life a plume of white steam rising from the roof, the afternoon sun gleaming off its glassy facade, it stares bleakly south, toward Washington, the White House, and the centers of national power.

All around sprawl the vast macadam parking lots for the 20,000 employees who work there. They have passed some of the most rigorous security tests in the Government, but they may be fired merely on a suspicion. They are enjoined from talking even to their spouses about their work. And inside the building they are physically restricted as well. The colored badge each of them wears tells the patrolling Marine guards into which areas they may and may not go.

Their work is of two kinds. Some of them protect American communications. They devise cryptosystems. They contract for cipher machines, sometimes imposing performance standards so high and tolerances so close that suppliers quit in despair. They promulgate cryptologic doctrine to ensure that the procedures of, say, the State Department do not compromise the messages of Defense. But the main job is SIGINT—signal intelligence—listening in. To do all its work, the N.S.A. alone spends about $1 billion a year. The agency also disposes of about 80,000 servicemen and civilians around the world, who serve in the cryptologic agencies of the Army, Navy and Air Force but stand under N.S.A. control, and if these agencies and other collateral costs are included, the total spent could well amount to $15 billion.

The N.S.A.'s place on the organizational chart is ambiguous: It is "within but not a part of" the Defense Department. The Secretary of Defense merely serves as the "executive agent" of the President in carrying out the functions assigned to the agency. It is not subordinate to the C.I.A., but its director sits on the United States Intelligence Board, the intelligence community's steering committee, whose chairman is the Director of Central Intelligence—the C.I.A. chief. The N.S.A. director is always a three-star general or admiral. (The deputy director must be a career cryptologist.) The President appoints the director, rotating among the three services, which get 85 percent of its output. The seven directors before General Allen held the job for an average of three and a half years each.

The agency's orders—Truman's 1952 directive—are to "obtain foreign intelligence from foreign communications or foreign electronic signals," General Allen is said to have told the House Intelligence Committee. The agency can be remarkably successful.

"Most collection agencies give us history. The N.S.A. is giving us the present," said Lieut. Gen. Daniel O. Graham, a former head of

the Pentagon's Defense Intelligence Agency (D.I.A.). "Spies take too long to get information to you, [satellite] photographs as well. N.S.A. is intercepting things as they happen. N.S.A. will tell you. 'They're about to launch a missile. . . . The missile is launched.' We know in five minutes that a missile has been launched. This kind of intelligence is critical to the warning business."

During the Strategic Arms Limitation Talks (SALT) of 1972, the N.S.A. reported on the precise Soviet negotiating position and on the Russian worries. "It was absolutely critical stuff," said one high intelligence officer. The information was passed back quickly to the American diplomats, who maneuvered with it so effectively that they came home with the agreement not to build an antiballistic missile defense system. "That's the sort of things that pays N.S.A.'s wages for a year," the officer said.

In 1973, large antennas appeared in satellite photographs of Somalia, which lies east of Ethiopia on the Indian Ocean. They looked like Soviet models. But not until the N.S.A. had learned where the antennas' signals were going to and coming from was the Government certain that the Russians, who had been kicked out of Egypt, had moved their military advisers into Somalia in force and were controlling their warships in the Indian Ocean from there.

Examples like these made General Allen's task a little easier when he appeared before the Senate Intelligence Committee. Senator Walter F. Mondale, the Minnesota liberal, told the general, "The performance of your staff and yourself before the committee is perhaps the most impressive presentation that we have had. And I consider your agency and your work to be possibly the single most important source of intelligence for this nation."

Senator Church concurred. "We have a romantic attachment to the days of Mata Hari that dies very hard. The public has the impression that spies are the most important source of information, but that is definitely not so. The more authoritarian the Government being penetrated, the less reliable the information derived from secret agents. In the Soviet Union and other Communist countries, the penetrations are likely to be short-lived and the information limited. But information obtainable through technical means constitutes the largest body of intelligence available to us, except by overt means."

And, he might have added, the most reliable. It is free of the suspicion that blights a spy's reports: Is he a double agent? Photographs from satellites also provide data as hard as can be, but, as Schlesinger once remarked, "nobody has ever been able to photograph intentions."

On the other hand, communications intelligence is far more easily jeopardized than other forms of information gathering. If a Government merely suspects that its communications are compromised, it does not have to hunt down any spies or traitors—it can simply change codes. And this will cut off information not from just one man but from a whole network. That is why the Government is so hypersensitive to any public mention of the N.S.A.'s work. When President Ford last September refused to send classified material to the House Intelligence Committee after it made public four apparently innocuous words—"and greater communications security"—it was because of fears that the words would reveal to the Egyptians, to whom they referred, that the United States had pierced deeply enough into their

communications to detect important changes. When last February he invoked executive privilege for private firms to keep them from furnishing information to a House committee looking into Government interception of private telegraph and teletypewriter messages, it was also for fear of compromising N.S.A. procedures.

In doing its work, the agency doesn't just tune up its receivers and go out hunting for codes to break. It gets its assignments from other elements of the Government. They tell the United States Intelligence Board what information they need that the N.S.A. can probably provide. After board approval, the Director of Central Intelligence levies the requirements upon the N.S.A. Typical assignments might be to locate and keep track of all the divisions of the Chinese Army, to determine the range and trajectory of Soviet ICBM's, to ascertain the characteristics of radars around East Berlin. In all of these, the first step is to seek out the relevant foreign transmissions.

Some of the intercepts come from N.S.A. teams in American embassies. The team in Moscow has been spectacularly successful—at least before the Russians began flooding the building with low-intensity microwave radiation. It had picked up the conversations between Soviet leaders in their radiotelephone-equipped automobiles and other officials in the Kremlin.

More intercepts come from special satellites in space called "ferrets". Swinging silently over the broad steppes and scattered cities of the Communist world, or floating permanently above the golden deserts and strategic gulfs of the Middle East, these giant squat cylinders tape-record every electric whisper on their target frequencies. These they spew out upon command to American ground stations.

Most radio intercepts come from manned intercept posts. Some of these are airborne. The Air Force patrols the edges of the Communist block with radio reconnaissance airplanes, such as the supersonic SR–71, the EC–135, and the EC–121, which carries a crew of 30 and six tons of electronic equipment. These planes concentrate not on communications intelligence (COMINT) but on the second branch of signals intelligence—electronics intelligence, or ELINT.

ELINT plays an important role in modern war. Suppose the Air Force were to send a bomber force against Moscow. Soviet radars would detect the force and report its range, direction and speed, enabling their fighters to attack. To delay this, the Americans would have to jam the radars, or "spoof" them—i.e., emit counterfeit pulses that would indicate a false position and speed for the bombers. But to do this, the Air Force would first have to know the frequency, pulse rate, wave form and other characteristics of the Russian radars. That explains why, in fiscal 1974, according to a report of the Center for National Security Studies in Washington, the Air Force flew at least 38,000 hours of ELINT flights—better than a hundred hours a day—dissecting radar signals with oscilloscopes and other electronic means. The game is not without its risks. No nation leaves all its radars turned on all the time. So the planes sometimes dart toward the country's territory. They hope the target will turn on its more secret radars. The danger, particularly at a time of international tension, is that the target will take the tease for the real thing and start World War III.

Other N.S.A.-directed posts lurk in the depths of the sea, aboard submarines in the Navy's Holystone program. This seeks, among other things, to "fingerprint" the acoustics of Soviet missile submarines. Aboard the Holystone submarine Gato, when it collided with a Russian sub in the Barents Sea in 1969, were eight sailors working for the Navy's N.S.A.-related security group. The Navy also used to have nine noncombatant surface ships collecting signal intelligence. But after the Liberty was strafed by Israeli forces during the Six-Day War of 1967 and the Pueblo was captured by the North Koreans, it decommissioned this mode.

The vast majority of the manned posts are fixed on the ground. They ring the Soviet Union and China—clusters of low huts huddling on a dusty plain or in the foothills of some remote Karakoram. In Turkey, they nestle close to the Russian underbelly. The post at the Black Sea port of Sinop—the ancient Sinope, which centuries ago colonized the shores of the Euxine—strains to hear Soviet voices. At Okinawa, the antenna field cobwebs a mountainside.

But much of the interception is done by servicemen. Earphones clamped to their heads, they hear the staccato of Russian Morse: One Soviet Army post reports the movement of half a dozen trucks to another. Other messages are in cipher. On a voice circuit, soldiers can be heard talking on maneuvers.

During moments of tension, the routine changes. Transmitters will vanish from their usual points on the dial. Station call signs will cease following their normal pattern of changes. Yet this is when information is most needed. The monitors hunch over their radio sets as they hunt up and down the frequency spectrum for their target transmitter. They can recognize him by peculiarities in sending or by the tone of his transmitter. One may sound like dowdydowdow, another like doodeedoodee. One may sound as if he's sending from inside a can; another may let his frequency slide up two or three kilohertz during a message.

They type out their intercepts on four-ply carbon paper and pass them back to the analysts. These men graph message routing to deduce organizational relationships. They monitor traffic volume for an upsurge that might indicate unusual activity. They extract from the message content indications of equipment capabilities, unit morale, names and characteristics of commanders. And they send the messages in cipher back to the cryptanalysts.

These are the aces, the shamans, of the communications intelligence business. They are the descendants of the ruffed divines and mathematicians who broke codes in curtained, candle-lit black chambers to further the grand designs of their absolute monarchs. The N.S.A.'s modern Merlins work in large open spaces filled with rows of gray steel desks. They pore over green-striped sheets, tap on computer terminals, print letters with colored pencils in rows and columns on cross-ruled paper, sip coffee, confer. Their successes become the agency's most jealously guarded secrets.

They succeed, however, mainly with the ciphers of third-world countries and with the lower-level ciphers of major powers. Underdeveloped nations have neither the money nor the expertise to secure their messages from American—and Russian—exposure. Anyhow,

they mainly want to keep things secret from their neighbors—Pakistan from India, Egypt from Israel, Argentina from Chile. So they buy commercially available cipher machines. But N.S.A. cryptanalysts, backed up by probably the largest concentration of computers under one roof in the world, some of them perhaps a generation or two ahead of any others in existence, can often beat these.

The major powers, on the other hand, use machines to generate ciphers so strong that, even given a cryptogram and its plaintext, and all the world's computers of this and the next generation, a crypt-analyst would need centuries to reconstruct the cryptosystem and use the reconstruction to read the next message. The N.S.A., in other words, cannot get the most desirable communications intelligence—the high-level messages of the Soviet Union and Communist China. (The SALT coup was partly the result of a Soviet enciphering error.) Worse, the area in which cryptanalysts may expect success is shrinking. The main reason is the declining cost of computation. This is falling by 50 percent every five years; the most obvious example is the price of pocket calculators. For the same amount of money as it spent five years ago, a nation can buy a cipher machine today with double the coding capacity. But doubling the coding capacity squares the number of trials the cryptanalyst has to make. Very quickly this work rises beyond practical limits.

So the N.S.A. asks for help. The F.B.I. burglarized embassies in Washington for it. The C.I.A. has subverted code clerks in foreign capitals: It once offered a Cuban in Montevido $20,000. In 1966, it bugged an Egyptian code room to pick up the vibrations of the embassy's cipher machines. The N.S.A., which could not cryptanalyze this machine, though it was commercially available, analyzed the recordings, revealing the machine's settings—and hence the messages. The C.I.A.'s most spectacular assist came in 1974, when it spent $350 million in an unsuccessful secret effort to raise a Soviet submarine from the depths of the Pacific, with missiles and cipher machines intact.

In room 6510 at the State Department, the intercepts come in on white sheets of paper bearing the heading "To Secretary of State from DIRNSA [Director, N.S.A.]." Several lines of gibberish indicating the distribution are followed by the text of the intercept, unscrambled on the spot. R.C.I. officers (for "research—communications intelligence"), one for each geographic area, insert the new material into fat loose-leaf binders and pull out the old. Once a week or so, the country directors mosey on down to room 6510 and leaf through the file to keep current with their areas. If something urgent comes in, the R.C.I. officer calls the country director, who comes right down. Daily, an R.C.I. officer conceals the more important intercepts under black covers (the C.I.A.'s color is red) and carries them in a briefcase to the several Assistant Secretaries of State.

Dramatic intercepts are rare. And when they come, they seldom have much impact. Once, an intercept arrived suggesting that a *coup d'etat* could take place in a certain country in a matter of hours. It was rushed to U. Alexis Johnson, then Under Secretary of State. He read it, nodded, said, "That's interesting," and handed it back to the R.C.I. officer. There was simply nothing he could do about it.

The vast majority of the intercepts are low-level routine. At State, they deal largely with the minutiae of embassy business, such as foreign

messages dealing with Soviet visa requests to foreign governments, reports of foreign ambassadors about meetings with American officials, foreign businessmen's orders. At Defense, they may include foreign ship locations, a reorganization in a Soviet military district, the transfer of a flight of Iranian jets from Teheran to Isfahan. Nearly all come from third-world countries. Usually they are of secondary interest, but sometimes their importance flares: Korea, the Congo, Cuba, Chile. And since these countries are spoken to by the major powers, their messages may carry good clues to the major powers' intentions. (This was another of the sources for the SALT intelligence.)

The quantity is enormous. In part this reflects the soaring increase in communications throughout the world. In part it marks a shift to the more voluminous peripheral sources, such as observing message routings, to compensate for the growing difficulty of cryptanalysis in areas of central interest, such as Russia and China. Unfortunately this overwhelming volume can stifle results. In late September 1973, just before the start of the Yom Kippur War, "the National Security Agency began picking up clear signs that Egypt and Syria were preparing for a major offensive," the House Intelligence Committee reported. "N.S.A. information indicated that [a major foreign nation] had become extremely sensitive to the prospect of war and concerned about their citizens and dependents in Egypt. N.S.A.'s warnings escaped the serious attention of most intelligence analysts responsible for the Middle East."

"The fault," the committee concluded, "may well lie in the system itself. N.S.A. intercepts of Egyptian-Syrian war preparations in this period were so voluminous—an average of hundreds of reports each week—that few analysts had time to digest more than a small portion of them. Even fewer analysts were qualified by technical training to read raw N.S.A. traffic. Costly intercepts had scant impact on estimates."

If N.S.A. failed in this major test, how does it do in its day-to-day operations?

A survey at the State Department showed that most desk officers felt that while the N.S.A. material was not especially helpful, they didn't want to give it up. It made their job a little easier. A former top State Department official was always glad to see the man with the locked briefcase. "I got some good clues on how to deal with various countries," he said, "and I quickly learned which ambassadors I could trust and which not."

At the Defense Department, most officials said they appreciated the help they got from the agency. "D.I.A. relies very heavily on N.S.A.," said General Graham, "because D.I.A. puts out a warning document to American units all over the world and to Washington, and whether the warning lights are green or amber or red comes mostly from the N.S.A."

For policy makers, naturally, the more information the better. But is this marginal advantage worth the billions it costs in a nation that has so many other vital human needs unfulfilled? Put that way, the question poses a false dilemma. The money for health and housing and education can—and should—come from elsewhere. It is on the vastly larger arms budget, on atomic overkill and obsolescent nuclear aircraft carriers, that the nation overspends. Intelligence is far cheaper and

usually saves more than it costs. In general, with its record of some failures and some successes, and the incalculable potential value of its sleepless watch around the world, the N.S.A. is worth the money the nation spends on it.

The real question for a nation reappraising its intelligence community is not one of financial priority but of legal basis. There is no statute prohibiting the N.S.A. from activities that encroach on Americans' constitutional rights. In response to criticism, President Ford recently issued an executive order on intelligence that seems to forbid the N.S.A. from intercepting American communications—but also seems to leave a loophole. Even with the best of intentions, however, that cannot be an adequate approach. For what one President can order another—or even the same—President can abrogate or amend.

The final responsibility for all those improper activities by the N.S.A. was, in each case, the President's, even though it remains unclear whether all of them were reported to the Oval Office. That alone should illustrate the hazards of an arrangement under which the powers of an intelligence service derive not from Congress but from the White House. As a basic reform, Congress should replace Truman's 1952 directive with a legislative charter for the N.S.A.

That, in fact, was the view that underlay much of the questioning of General Allen before the Senate Intelligence Committee; and that is the substance of the recommendations on the N.S.A. contained in the committee's recent report on the intelligence establishment as a whole. "The committee finds," said the report, "that there is a compelling need for an N.S.A. charter to spell out limitations which will protect individual constitutional rights without impairing N.S.A.'s necessary foreign intelligence mission." The committee also made specific recommendations designed to prevent a repetition of the known abuses of the past.

The House Intelligence Committee, in its own report, came to the same basic conclusion, declaring that "the existence of the National Security Agency should be recognized by specific legislation," which should "define the role of N.S.A. with reference to the monitoring of communications of Americans."

There is no question that the National Security Agency, in the words of the Senate committee report, is "vital to American security." In fact, in this nuclear age, when danger-fraught situations can be best handled with knowledge about the "other side," and when many international agreements, such as SALT, are dependent on, say, America's ability to verify Soviet compliance by its own technical means, N.S.A. intelligence, like all intelligence, can be a stabilizing factor in the world.

There is also no question that we need a new statute. No law can guarantee prevention of abuses, especially if lawlessness is condoned in the higher echelons of government, and the C.I.A.'s charter did not prevent that agency from overstepping its bounds. But a gap in the law is an invitation to abuse. An institutionalized mechanism to seek out violations and punish the guilty can best deter the sort of intrusion that so many Americans fear—and that destroys the very freedom the N.S.A. was created to protect.

[From the Washington Star, Aug. 12, 1976]

Church of Scientology Finally Gets Foothold on NSA

DATA YIELDED GRUDGINGLY UNDER INFORMATION ACT

(By Vernon A. Guidry, Jr.)

The National Security Agency is the kind of operation in which the public affairs office telephone is answered with a four-digit number rather than a name, a practice that even the CIA has abandoned.

So perhaps it wasn't surprising when NSA time after time told the Founding Church of Scientology of Washington that it could find no information in its files about the church, nor its founder, L. Ron Hubbard.

The church had made repeated requests over a number of months, asking NSA under the Freedom of Information Act if that massive electronic spy agency had any such information.

The church was no stranger to the federal government's investigatory and information gathering arms, nor to controversy, most of which centered over the use of a lie-detector like device called an E-meter to assess the mental and spiritual condition of a subject.

But of late, the church has been striking back at the FBI, the Internal Revenue Service, the CIA and the NSA, chiefly through the courts and the information act.

While it was carrying on a game of thrust-and-parry with NSA through the mails, the church was also suing the CIA. In the course of that suit, the CIA admitted that it had 16 documents relating to the church in its files—all received from NSA.

Armed with that information, the church went back to NSA this June and demanded once again that the agency own up to having information in its files.

This month, the reply from NSA was received. Yes, the agency acknowledged that it had found at least 15 of the 16 documents identified by the CIA. But it still claimed that the earlier denials were accurate.

That claim was made in a letter to the church from John R. Harney, who identified himself as a "freedom of information appeal authority."

Harney wrote that the documents "were located in warehouse storage and were found only on the basis of the information we received from the CIA; they could not be found on the basis of the subject matter content.

"I must therefore reaffirm the NSA information officer's previous statements that no information was located in agency files concerning the Church of Scientology under any of the headings or in each of the categories, as specified in your previous requests, in this agency's records," Harney wrote.

In any event, would NSA now release the documents, whatever they are? No. Wrote Harney: "The National Security Agency is precluded by Title 18 U.S.C. 798 from providing information concerning classified communications intelligence activities except to those persons authorized to receive such information."

That admission didn't go unnoticed by the scientologists. A spokesman, the Rev. Hugh Wilhere, declared that "the fact that the NSA is holding files and conducting 'foreign intelligence activity' on a church by their own admission is highly incriminating in itself."

There are those in NSA who apparently would like to say more in their own defense on this issue. Information officer Norman Boardman, who was involved in some of the correspondence that assured the church that no such documents existed, is one of them.

Yesterday, Boardman was asked how, for instance, the CIA could find the documents supplied by NSA, but NSA could not. While supplying no direct answer, Boardman insisted that "there are two sides to this thing."

When a questioner on the telephone asked him to expand on that, he said he would call back. When he did, he said only, "I'm not prepared to go beyond 'no comment.'"

True to the form it has been developing, the church yesterday went to court. It filed a Freedom of Information action in U.S. District Court here to force release of the documents.

And, it asked the court to force NSA to make a search of its records, a complete search this time.

[From the Washington Star, Sept. 10, 1976]

In Focus

Two Satellites Revolutionize the Way We Map the Earth

CHARTS NOW TELL VASTLY MORE THAN HOW TO GET THERE

It would not be surprising if in this one program alone the nation would realize a return exceeding its total space program investment.

—Werner Von Braun on the Landsat mapping satellite program, 1971.

(By Thomas Love)

Maps and mapping techniques really didn't change all that much during the several centuries before World War II.

Of course, accuracy increased—it didn't take too long to determine that California really wasn't an island. And printing methods improved—high speed presses replaced hand copying—but the basic methodology and end result stayed pretty much the same.

During the past few decades, however, things have changed drastically.

For instance:

Maps have been developed which can be used to update census data through land use alterations observed by a satellite 570 miles above the globe.

Vehicles used in mapping have self-contained internal navigation systems that sense and record not only the vehicle's every twist and turn but its changing altitude.

Aerial photographs of the earth's surface, which have supplanted most tedious ground surveying, are projected in midair to form a three-dimensional picture that is used to determine altitudes for maps.

Full-color maps of large areas can be "drawn" in just minutes from satellite-gathered data stored in a computer.

Maps are being produced which can predict the success or failure of a crop long before harvest time, help inventory forest products and show previously unsuspected geological features.

Two U.S. Government agencies are at the heart of this major change in cartography—the National Aeronautics and Space Administration and the U.S. Geological Survey. Together, they are revolutionizing the art.

NASA's contribution comes from its high-altitude aerial photography activities and its two mapping satellites, Landsats I and II, soon to be joined by the more sophisticated Landsat III.

Since the USGS conducts nearly all of the basic mapping in this country, it is the No. 1 NASA customer.

Von Braun's optimistic view of the economic impact of the Landsat project may not yet have been proven correct, but in one way, at least, Landsat I was a bargain for taxpayers—it was launched in 1972 with a projected useful life of one year. It's still working fine and sending back useful data today.

The two satellites, which cost some $197 million, are actually research and development vehicles for NASA. According to Alex Tuyahov of NASA's User Affairs Division, they "were launched to find out what you can do with this new view from space."

The satellites—they're carbon copies—look at the earth with four "eyes" that record the visible colors red and green as well as two frequencies of infrared radiation. Landsat III—now Landsat C since satellites switch from alphabetical to numerical designation upon launch—will add a fifth heat sensing detector.

As the satellites spin around the globe, they are constantly monitoring what they see in the four frequencies of radiation and relay that information to earth.

Each passes over every point on earth once every 18 days. The orbits have been set, however, so that every point is monitored every nine days by one of the pair.

The data is returned to earth not in any visual, map-like form, but as a continuous series of numbers that tell the amount of reflected light recorded in each of the four monitored frequencies.

For instance, if a certain point reflects no green light, the satellite will report what amounts to a zero for that frequency. The more the green, the higher the number.

The satellites return a report on every 1.1-acre plot on the face of the earth, the smallest section they can "see."

All this data is relayed to the Geological Survey's data center in Sioux Falls, where it is available to anyone who has any use for it—domestic or foreign.

There is such a demand for Landsat data that a number of foreign governments have set up their own ground receiving stations. The only provisions that NASA demands are that the information must

be made available to anyone and that the receiving government must sell it at cost.

The possible uses for all this information are almost endless. By making various combinations of the data in the four frequencies, mapmakers, or cartographers, can determine an amazingly detailed picture of the earth.

For instance, James R. Wray of the USGS headquarters in Reston has used similar data from lower-level aerial photographs to develop a series of experimental maps of the Washington area, which show land uses and land-use changes over a period of time.

One set of maps shows the area in 1970, a census year, and two years later. They show that between the two dates there was a 4.6 percent increase in land devoted to multi-family housing, a 0.4 percent increase in single-family housing and a 2.2 percent drop in open space.

The 1972 map shows the construction of the Mormon Temple in Silver Spring, the destruction of the old Navy tempos along the Mall and the draining of Lake Barcroft in Fairfax County after its dam abutment was washed away during Hurricane Agnes.

Such maps could be used to update population data between the regular 10-year census counts, inventory land-use trends for local control measures and shown growth patterns before they become obvious from other sources.

Each of the maps was made from two sets of photographs taken several months apart for added accuracy. For instance, a freshly cut barley field looks like a house roof. A check of the field during a different time of the year would show it to be barley, not a roof.

Satellite data can be very detailed. It can show the difference between new and old residential areas; silver fir and douglas fir trees; healthy, vigorous crops and infected or stunted plants.

The Government is now working on a program using such maps to help the Soviet Union check on its current corn crop.

With proper programing, the computerized satellite data be sent through a film recorder to automatically create a color map.

However, most of the USGS cartographic activities deal with less exotic mapping.

According to Robert H. Lyddan, chief of the Topographic Division, "the U.S. has been little interested in mapping. As a result, we are now at the point England was 100 years ago. It is only recently that the general public here has become very much concerned."

Because of military interest, he continued, Germany and France were far better mapped at the outbreak of World War I than this country is today. The excellent maps now commonly used in Britain are more than a century old.

Serious modern mapping began in the United States with the creation of the Tennessee Valley Authority in 1933, he said. There was further impetus as World War II approached and there was fear that domestic maps might become a military necessity.

The survey is still trying to complete mapping the entire "lower 48" states with 1:24,000 large scale maps in which one inch represents 2,000 feet on the ground.

Only about 80 percent of the country has been mapped at that scale for the older 1:63,360 scale, in which one inch equals one mile. There are no plans to map Alaska at 1:24,000, only at 1:63,360.

The only maps which cover the entire nation are in a 1:250,000 scale in which one inch equals about four miles. At this small scale, little detail can be included in the map.

With the planned changeover to the metric system in the United States, the Geological Survey faces the additional challenge of having to redo all its maps in the new measurement. Although much of the same data can be used in the metric 1:25,000 scale maps, all altitudes will have to be redone in meters rather than feet.

This doesn't pose any great problem for such points as mountain peaks. But all the contour lines, a continuing line which connects all points of the same altitude, will have to be redone in meters—not a minor project.

The first of the new metric maps are being prepared for the Lake Placid area of New York. The Survey plans to have the project finished by the time the next winter Olympics are held there in 1980.

Although the basic topographic map of today doesn't look too different from those of a few decades ago, the way they're put together is a far cry from previous methods.

Once, a map was drawn almost entirely from information actually gathered on the ground. Surveyors walked through the area, measuring distances, recording angles, noting the location of streams and roads, checking altitudes and making voluminous notes on what they found.

Things have changed.

Now when a new map is planned for an area, the exact location and altitude of several key points is determined on the ground. Even this is often done differently than before with sophisticated distance measuring equipment utilizing such new developments as lasers.

Then two aerial photos are taken of the area. They are exposed a specific distance apart from a plane flying along a predetermined course at a specified altitude. Transparent prints from these pictures are placed into double-projection in the same orientation as when they were taken.

This machine is a distant relative of the old parlor stereoscope that produced a three-dimensional picture from two photos taken from slightly different angles.

With the map-making machine, the cartographer sees a clear three dimensional projection of the land to be mapped floating above his tracing table. From this, the details from the photographs are traced on the base of the tracing table.

To get the contour lines, he sets a marker on a vertical instrument at a certain altitude—determined from the preselected points—and draws around what he sees as hills and valleys. These lines are recorded on the map table and become contour lines.

Ironically, the satellite photos that have been such a boon for so many aspects of map making can't be used for these large-scale maps. "They just aren't detailed enough for the 1:24,000 maps we're making now," Lyddan said. "It's too bad they weren't around 100 years ago when we were making small-scale maps."

[From the New York Times, Sept. 13, 1976]

Growing Use of Electronic Warfare Is Becoming a Source of Major Concern for World's Military Powers

(By Drew Middleton)

Electronic warfare, a sophisticated and expensive complex of technological weaponry, is rapidly becoming a major military preoccupation of defense establishments of the United States, the Soviet Union and the North Atlantic Alliance.

The advantage in the use of electronic warfare lies with the side that is best able to deceive or suppress high technology weapons systems such as air-to-surface missiles.

"We will throw an electronic blanket over their air defenses that will allow our aircraft to attack without danger from anything more than lucky shots," said Col. James L. McKenna. He directs an Air Force program at the Wright-Patterson Base in Ohio where the BF–111A is being developed into an electronic warfare escort plane for tactical strike missions.

Maj. Gen. E. S. Frits of the Marine Corps recently told a Senate subcommittee that "an electronic-warfare capability is an absolute requirement for survival in any future conflicts."

NATO SCANNERS JAMMED

The Warsaw Pact's achievement during the invasion of Czechoslovakia in 1968 exemplified the defensive use of electronic warfare. The Soviet Air Force scattered a vast amount of aluminum foil or chaff along the frontier and the movement of Soviet ground and airborne units into Czechoslovakia went almost completely undetected by NATO's electronic scanners.

Electronic warfare is a highly secret field. But some estimates of investments in it have become available recently from authoritative sources. One is that the United States, the Soviet Union and Western European states will spend about $1 billion this year on procurement of equipment for electronic warfare and approximately as much on research, development, testing and evaluation of new systems. According to an authoritative European source, the United States will spend $780 million for procurement and $339.1 million for research and associated program.

A European expert defined the three basic objectives of electronic warfare as:

To use all the electromagnetic radiation released intentionally or accidentally by an enemy.

To interfere with enemy use of the electronic equipment to a degree that renders it ineffective or even dangerous to the enemy.

To defend a force's own use of electronic equipment.

Both the Soviet Union and the United States are seeking these goals with the Russians, at the moment, concentrating on the mass use of chaff. Qualified American sources believe that, in the event of invasion of Western Europe, the Soviets would spread chaff to cover the corridors used by advancing air and ground forces.

The United States and its allies appear to concentrate on more subtle, less widespread tactics aimed at blotting out the radar and guidance systems of Soviet missile sites, airfields and antiaircraft weapons.

Radar, the handmaiden of missiles, guns and combat aircraft, is the target for electronic warfare on both sides. Every radar can be identified by its "signature."

This signature consists of measurable elements including transmission frequency, power, pulse width and pulse repetition.

The United States services use electronic intelligence systems in seeking to collect and analyze all of a prospective enemy's electromagnetic emissions from land-based, airborne or naval radars.

Electronic intelligence systems can span each frequency band continuously, analyze each signal, determine the signature and compare it with others for identification and location.

[From the New York Times, Dec. 22, 1973]

Little Adjustment Needed on Improved TV Camera

(By Stacy V. Jones)

Washington, Dec. 21.—A new color television camera, patented this week for the Columbia Broadcasting System, is described as a significant advance in the art and as promising high performance. William E. Glenn Jr., vice president and director of research at C.B.S. Laboratories, Stamford, Conn., was granted Patent 3,780,212 for the camera and filter. The camera has a single image pick-up tube instead of the three now used in most color cameras to derive separate signals for the three primary colors.

Several other single-tube systems have been invented, but Dr. Glenn believes his overcomes disadvantages that they offer.

The Glenn filter has three sets of parallel stripes. Yellow, cyan (dark blue) and magenta stripes are used to produce the complementary colors: red, green and blue.

The new camera requires little adjustment, and if there is some accidental misadjustment the color is changed very slightly. C.B.S. will probably license a manufacturer to produce it.

Among Dr. Glenn's other inventions for C.B.S. is a process for recording and reproducing information from microfilm. For the General Electric Company, a previous employer, he patented a television projector and a television recording process.

BAGGAGE X-RAY SYSTEM

The Microdose X-ray system, which is widely used by airlines to inspect baggage, was patented this week for American Science and Engineering, Inc., Cambridge, Mass.

Jay A. Stein and Roderick Swift were granted Patent 3,780,291 for what is technically called radiant energy imaging with scanning pencil beam.

The beam moves from top to bottom as a package being scanned moves from left to right. An X-ray detector behind the package produces electrical signals that display its image on a television picture tube. As illustrated in the patent, the image discloses a revolver.

American Airlines and Trans World Airlines are among the users. The radiation levels are said to be so low that the operators receive less radiation than the average jet pilot gets from flying at high altitudes.

The same system could be adapted for inspecting people, although the airlines now use other methods. The pencil beam can make a series of horizontal scans across a body, shifting downwardly. The beam level need not be changed if the subject is an airline passenger mounting steps.

[From the New York Times, Jan. 19, 1974]

Way To Speed Up Taped Speech Legibly Is Devised

(By Stacy V. Jones)

Washington, Jan. 18.—Variable Speech Control, which was patented this week, is designed to enable people to listen as fast as they read. The electronic device permits words to be played back at twice the rate they are delivered, without the usual Donald Duck effect. Murray M. Schiffman, an electronics engineer and inventor, was granted Patent 3,786,195.

The owners of the patent include Sanford D. Greenberg, a Washington businessman who has recovered from blindness, and the Cambridge Research and Development Group, Westport, Conn.

Licenses to incorporate the invention in tape recorders and cassettes have been granted to the Magnetic Video Corporation, Farmington, Mich., and two large Japanese manufacturers, the Sony Corporation and the Matsushita Electric Industrial Company, Ltd.

On the average, it is said, people speak only about half as fast (150 to 175 words a minute) as they read (250 to 350 words a minute). The device is expected to benefit the blind, who must usually listen to taped speech at its rate of delivery. Students can save time with recorded lectures. Broadcasters are expected to be able to speed up stock and sports reports.

Without altering the waveform, pitch or tone, the little device can not only compress speech but expand it for those who must listen more slowly.

The advantages of Variable Speech Control over previous equipment offered for the purpose are said to be its small size and low cost and the fact that the user can vary the playback speed at will.

[From the New York Times, Mar. 30, 1974]

First Major Change Made In Color TV Tubes by RCA

Washington, March 29.—The RCA Corporation this week received Patent 3,800,176 for the company's only major color tube design change since it manufactured the first color television sets exactly 20 years ago. The system eliminates many complex circuit components and cost-

ly, time-consuming color tube alignments at the factory and by the service man. The inventors are William H. Barkow and Josef Gross, members of the technical staff of the RCA materials and display devices laboratory in Princeton, N. J. Their invention is used in the production of all-solid-state—tubeless—sets. It is claimed these are cheaper, lighter, simpler to operate, more reliable and give a brighter picture.

In conventional television receivers 12 convergence controls are required to insure that the three primary color images—red, blue and green—overlap over the whole viewing screen. Initial alignment and later adjustment of these controls is costly and requires special equipment and skill.

The new system provides automatic register of the three color images without the use of adjustable controls. This is achieved by a new configuration of the electron beams in the tube, by a new design of the deflection yoke on its neck and by building a high degree of precision into the system.

Marking the 20th anniversary of color TV, RCA announced that it would become the first domestic producer to manufacture only color TV receivers that are all solid state.

The new sets consume from 22.5 to 52 percent less energy than comparable tube-type sets.

* * * * * * *

BUCKET-BRIGADE ELECTRONICS

The U.S. Philips Corporation, Briarcliff Manor, N.Y., received this week a basic patent on charge transfer imaging devices, an important development for television cameras and other means of electronic picture storage.

Reissue Patent 27,951 is based on one granted in 1971, revised to make the claims commensurate with the disclosed invention. The inventors are Frederick L. J. Sangster and Kees Teer of Philips Gloeilampenfabrieken, N.V., Eindhoven, the Netherlands, with which U.S. Philips has invention agreements.

It is expected that charge transfer imaging devices will come into wide use both here and abroad in television cameras and electronic readers.

In these devices minute electrical charges representing separate bits of the picture are passed along a silicon wafer about the size of a quarter from one picture element to the next, similar to the passage of water in an old-fashioned bucket brigade.

Images are stored as electrical charges in the silicon wafer until electrical pulses are applied to cause the charges to be converted to a video signal. Besides television, expected applications of the principle are in computer and logic systems.

The American Institute of Electrical and Electronics Engineers has presented to Mr. Sangster its David Sarnoff Award "for the invention of the bucket-brigade delay line and ingenuity in finding new realizations and applications of this principle."

[From the New York Times, May 16, 1975]

A Scanning Device for Quick Checks of Credit Invented

Mountain View, Calif. (UPI).—The first holographic memory unit that can check a credit card holder's rating within three seconds is now being produced by a firm here.

"Airline ticketing operations, gasoline companies and any retail operations that have their own credit or other credit cards coming across the counter can use the device," said James J. Wilson.

Mr. Wilson, president of Optical Data Systems, Inc., which holds the first patent granted such a device, said several international hotel chains are now using the firm's holoscan 300 memory unit.

Several Las Vegas gambling casinos have also installed the credit card checking device. The casinos can tell if a gambler's credit is good—and can even make special notations that tell how large a marker the gambler is good for.

FAST AND ACCURATE

The laser beam at the heart of the device makes fast, accurate scanning possible. The system is miniaturized and permit 350,000 to 700,000 credit ratings to be put on a 30-foot strip of 35 millimeter film.

If a customer were to ask for lodging at one of the hotels using the system, the clerk would punch the credit card's number into a keyboard.

"Within three seconds the memory unit would search a file to see if your card had been designated a bad credit risk," Mr. Wilson said.

"If your card number is not in the memory, the clerk gets a 'thumbs up' and you proceed with the checking in ceremonies."

However, should your card be included in the file, the clerk would get a negative response and refuse to accept the card.

[From the New York Times, Aug. 9, 1975]

Computer Setup Links a Variety of Devices

(By Stacy V. Jones)

Washington, Aug. 8.—A computer system invented at the upstate medical center of the State University of New York in Syracuse can control or collect information from hundreds of widely separated devices.

Leo F. Walsh, instructor and assistant director of bio-electronic and computer sciences, was granted Patent 3,898,373 this week. A demonstration system, in operation at the center, controls medical research and administration equipment.

A variety of units, including blood pressure monitors, check-writers, cash registers, time clocks, thermometers, automatic lathes, card readers and printers can be connected in a factory, hospital, story or office with a single coaxial cable in daisy-chain fashion.

At the small central computer, selected devices can be addressed by their individual codes and instructed what work to perform or what data to supply.

Under its invention agreement with the university, the Research Corporation, a New York foundation, will license the system to industry.

[From the New York Times, Oct. 2, 1976]

Signature Verification by Computer

(By Stacy V. Jones)

Washington, Oct. 1.—Specialists in the research laboratory of the International Business Machines Corporation at Yorktown Heights, N.Y., have invented a new method and apparatus for signature verification.

As a person who wishes to register his or her signature signs the name, electrical recordings are made, showing the acceleration forces and the changes in the speed and direction of the pen point or pencil. In fact, the name is signed several times, and the recordings are analyzed for a final reference pattern.

When some other person claims the registrant's identity, the claimant's signature is also recorded, and the patterns are compared by computer.

Noel M. Herbst and John H. Morrissey, members of the research staff, were granted Patent 3,983,535 this week.

Their studies showed that when a person reached adulthood, the signature became automatic, and the changes in speed and direction cannot be intentionally copied. The new verification method is far superior to mere visual comparison of signatures, even by trained personnel.

The invention is not yet on the market, but it is highly regarded for future use. After small-scale experiments are completed, it will probably be tried as a means of regulating access to secured parts of buildings.

[From the New York Times, Apr. 3, 1976]

Frogman Detector

Enemy frogmen can be dangerous. Royal W. Eckstein Jr. of Indianapolis obtained Patent 3,947,838 for the Navy this week on an automatic detector to discriminate between swimmers and such things as floating logs.

An electro-optical sensor first views an object in the water. If its width and other aspects indicate a diver, the information is encoded and compared with stored reference scenes to determine whether it actually is a swimmer.

[From the New York Times, Oct. 6, 1976]

TECHNOLOGY

AN ERA FOR ELECTRON-BEAM MACHINES

(By Victor K. McElheny)

Electron-beam machines, people in the semiconductor industry expect, will in the years ahead carry electronic microcircuits much further into the realm of cost-cutting micro-miniaturization and, consequently, into a widening range of mass-market products with computer features.

In effect, the circuits produced by these machines would enable manufacturers to put a tiny computer into many ordinary products to improve their efficiency and make it easier for people to use them. For example, such electronic microcircuits could be used in many home and office appliances and automobiles, improving fuel utilization or regulating complex time schedules for say, cooking a meal, or using several appliances at once even in the owner's absence.

Leading manufacturers expect to begin installing the million-dollar electron-beam machines within a few months. The machines, designed and made in the United States and using the same principle as the electron-beam microscope that produces far greater magnification than traditional optical equipment, are expected to begin their careers modestly, by improving the precision and efficiency of some types of present generation production of electronic microcircuits.

* * * * * * *

Although such companies as Texas Instruments and the International Business Machines Corporation have pursued electron-beam technology intensely, the first machines to go into the open marketplace in the United States are based on designs licensed by Bell Telephone Laboratories to two manufacturers.

These are the Etec Corporation of Hayward, Calif., and the Extrion division of Varian Associates of Gloucester, Mass.

Etec, of which James Dao is president, has specialized in scanning-electron microscopes for laboratory use. Extrion, of which Dr. Peter Rose is general manager, has been producing ion-implantation equipment used by semiconductor manufacturers.

Etec was licensed last October and expects to ship its machines first. Extrion, licensed last April, expects to ship around November 1977.

The machine is known at Bell Laboratories as the Electron Beam Exposure System. A leader in its development was Donald R. Herriott. Like other electron-beam machines, the Electron Beam Exposure System is designed for key steps in the special type of lithography by which electronic microcircuits are built up on a base of ultrasilicon.

To create arrays equivalent to thousands of transitors and other electronic devices on an area smaller than a fingernail, layers of chemicals sensitive to light or other radiation are deposited onto the silicon, exposed to the rays like photographic print paper in a darkroom, and then etched with acids.

The sensitive materials consist of polymer chemicals that are either made less resistant to the etching by exposure, in which case they are

called positive resists, or hardened against the acids and called negative resists.

Scientists at Bell Labs, including L. F. Thompson, have developed both positive and negative resists for electron-beam machines.

According to George Indig of Bell Labs' patent law department, packages of designs for these resists have been licensed to many companies on the same nonexclusive basis used with the machines. A total market of about 50 machines, at a cost of almost $1.2 million, "might be the limit over the next several years," Mr. Indig said.

At first, the electron-beam machines are expected to concentrate on one step of semiconductor manufacture. This is the making of so-called master masks of chromium on glass. It is through intermediate or working copies of such masks that radiation, usually ultraviolet light, is beamed at the sensitive layers on the silicon.

The ultrashort wavelengths of the electron beam, less than a thousandth of the wavelength of ultraviolet light, permits greater precision in manufacturing. Eventually, it should also permit many more electronic functions to be squeezed onto a given area of silicon.

To reach this target, however, scientists and engineers will have to find ways to make individual microelectronic chips far faster than would be possible with present electron-beam machines.

These write their patterns onto a surface like a pencil, or the "gun," that builds up a television picture dot by dot, line by line, 30 times per second. For speedy manufacturing, a way of "floodlighting" through a mask is preferred.

The developers of Electron Beam Exposure System contend that they have simplified matters by combining an electron-beam that sweeps back and forth over a short path, only 128 micrometers, with a laser-aligned, motor-driven table that moves the beam-target.

The developers are certain that their system will grow more powerful with the development of more sensitive resist chemicals, brighter sources of electrons and faster allied computer processing of the data about where the beam is pointing at a given split second.

In the opinion of developers and marketers of the electron-beam technology, the imminent shipment of electron-beam machines may come none too soon.

They note the Japanese Government's commitment of more than $250 million to a consortium of Japanese electronic companies seeking a significant share in the next generation of electronic technologies.

[From the New York Times, Oct. 30, 1976]

Patents: Video Memory Is Used in Intrusion-Detection System

(By Stacy V. Jones)

Washington, Oct. 29.—A new intrusion-detection system has a video memory that records the principal aspects of the area being guarded, sounds an alarm when something unusual happens and reproduces any movements of persons and property, disclosing where an intruder may have hidden.

Two electronics engineers, Peter Mick and Donald Beck, were granted Patent 3,988,533 this week for the system, which they have named Visigard. Their company, Video Tek Inc. of Mountain Lakes, N.J., has made and sold 15 units since the project was begun in April 1974.

The inventors decided that existing intrusion equipment lacked the sophistication of modern science. Usually a guard was equipped with closed circuit television, and boredom often resulted after he watched it for a half hour. Mr. Mick and Mr. Beck set out to develop automatic equipment that simulated the human eye.

Their cameras scan many fixed points in the scene being protected and store the record. In subsequent scans, automatic comparison is made, and an alarm is sounded if there has been a disturbance. As many as 16 cameras may be used and the scanned points may exceed 16,000.

Part of the equipment permits any special portion of the field of view to be magnified and reproduced on a television monitor, showing movements that have taken place. A "map" of the alarm area may also be displayed. The inventors expect that their system will greatly reduce the number of uniformed guards required by industry.

The patent is assigned to Video Tek Inc. in which the inventors hold a substantial interest. Additional financing is planned.

[From the Washington Post, June 17, 1976]

Computer Security Weak, FEA Told

(By Donald P. Baker)

The Federal Energy Administration was told last summer that the Rockville firm with which it had contracted to computerize classified plans to combat the energy crisis had not met required security precautions.

A report by the General Accounting Office last July 15 called the FEA's decision to award the contract to Optimum Services Inc. (OSI) "neither prudent nor proper," but added that it would have been too costly to revoke the $7.7 million contract then because it already was in effect.

Earlier this week, a former OSI employee was convicted in U.S. court of tapping into the computer at OSI where the sensitive national plans were stored. In his defense, Bertram E. Seidlitz, 38, of Lanham, contended that he stole information from the computer to demonstrate lax security at OSI.

Seidlitz tapped into the OSI computer from an office in Alexandria, using a computer terminal, telephone and knowledge he had gained while working as deputy director of the FEA project at OSI.

Seidlitz, who said he had complained about the lack of proper security while employed at OSI, faces up to 10 years in prison for his conviction on two counts of wire fraud.

The GAO report last summer was prompted by protests from losing bidders who argued that the FEA had not required the winning bidder to meet the security standards outlined in the specifications.

The losing bidders also said that OSI should have been disqualified

because its board chairman is Texas oil millionaire Clint Murchison Jr.

The competitors, On-Line Systems Inc., and Remote Computing Corp., said OSI's bid should have been rejected because the winning firm would be processing "sensitive proprietary data necessary for regulating the petroleum industry and for effectively combatting the energy crisis."

The GAO said there was nothing in the FEA specifications that barred bids by persons with interest in the oil and gas industries.

What obviously bothered the GAO was the absence of adequate security. In a letter to FEA Administrator Frank G. Zarb, Comptroller General Elmer B. Staats said that while the protests were denied, "we did conclude that it was neither prudent nor proper to have waived the mandatory" security requirements.

James A. Spangenberg, the GAO attorney who wrote the report, said there was "lots of concern on the Hill because of Murchison."

The GAO was more concerned by the failure of OSI to meet "read protection requirements," Spangenberg said. He said the particular computers used by OSI would "need a lot of modification" to meet U.S. requirements to assure that unauthorized persons could not "read" classified material on the computer.

The OSI equipment met external security requirements, meaning that persons outside the firm could not plug into the computer, but it could not prevent employees (or in the example of Seidlitz, former employees) from gaining access to sensitive data, Spangenberg said.

"We did not regard this as a minor deficiency," Spangenberg said yesterday. He described the theft of information by Seidlitz as an "I-told-you-so."

The GAO said it rejected the complaints primarily because it would have cost the government more than $12 million to cancel the contract with OSI and award a new contract.

Instead, it advised the FEA to urge OSI to modify its equipment and upgrade the security.

The GAO report said "it is essential that FEA strictly limit access to the computer system to persons whose participation is necessary. We plan to monitor the system's operation to insure compliance with this standard."

The GAO asked the FEA to inform the agency about "action taken in response to its recommendations." But Spangenberg said yesterday the FEA has not replied.

In a letter to Zarb on April 8, acting comptroller general R. F. Keller said "despite the passage of seven months and numerous inquiries, we have not yet received any response to our letter."

[From the Washington Post, June 16, 1976]

Theft by Computer

Conviction Called Landmark

(By Donald P. Baker)

A Lanham man whose burglar tools were a computer terminal, a telephone and an extremely clever mind was convicted in U.S. court

in Baltimore this week of tapping into a computer that contained classified files of the Federal Energy Administration.

Punching secret passwords into a keyboard computer attached to a telephone in his Alexandria office, the defendant, Bertram E. Seidlitz, dialed the telephone number of the computer firm in Rockville where the FEA information was stored and extracted 40 rolls of computer printouts before he was caught.

U.S. Attorney Jervis Finney said the tapped computer contained classified data relating to oil and other energy resources of the nation. The federal prosecutor said the computer-age theft "signals the future of white-collar crime."

Stan Neeley, president of Optimum Services Inc. (OSI), the Rockville firm that has a $7.3 million annual contract to provide computer services to the FEA, said the information Seidlitz obtained was valuable not because it divulged FEA secrets but because it would permit computer firms to duplicate the complex system used to store the FEA data.

Neeley said the conviction was a "landmark" in the computer industry, "which needs to find a method to protect its assets from theft."

Seidlitz, 38, of 8629 Brae Brooke Dr., Lanham, admitted the theft but he said he did it only to show how lax security was at OSI, where he formerly was employed.

Meeley said OSI, which has 1,300 employees throughout the country, is a large federal contractor that also performs computer work for the Federal Trade Commission, Environmental Protection Agency and the Departments of State and Labor.

Neeley said the only reason Seidlitz was able to tap into the computer was because he was a former employee "who retained in his memory the keys to unlocking information."

The computer fraud was discovered by an OSI employee who was monitoring the computer and "detected an unauthorized user on the line accessing the computer," Neeley testified at the trial, which ended Monday.

The trial, before U.S. District Court Judge Alexander Harvey II, lasted eight days. Because much of the testimony was offered in computer jargon, much time was spent translating the technical terms into words the jurors could understand.

Defense attorney Frank M. Kratovil of Hyattsville argued that Seidlitz wanted to show "in good faith" to the FEA that OSI's computer "could be accessed."

From Oct. 19, 1975, through Jan. 9, 1976, Seidlitz secretly withdrew from the OSI computer 18 of the 20 codes needed to extract information from the Wylbur program and its companion program, Milton, which are used by OSI to store the FEA data. (The programs were developed at Stanford University in the mid-1960s, and were named for the Wright brothers and their father, according to Neeley. The third program, Orville, was not involved in the theft.)

OSI, whose national headquarters is in Santa Clara, Calif., bought Wylbur, Orville and Milton Computer systems from Stanford, and Neeley testified the company spent $100,000 improving them.

The sophisticated systems give OSI a competitive edge that has resulted in $30 million to $40 million in contracts, Neeley said.

Roger Fajman, one of the original designers of Wylbur at Stanford and who now is a computer specialist at the National Institute of Health, testified for the defense. His testimony indicated that it would have been difficult for Seidlitz to convert the Wylbur program for use with the computer that Seidlitz' company rents.

The system is valuable because of its ability to handle more users than some competitive systems, and because it responds to simple commands that makes it easier for novices to operate, Fajman explained.

When the OSI employee detected the unauthorized user of the line last Dec. 30, company officials contacted the C & P Telephone Co., which traced the call to Seidlitz' computer firm in Alexandria.

The next day, the unauthorized user was back at work, tapping the computer, but that time, OSI got a duplicate printout, which it gave to the FBI.

Using a court ordered search warrant, the FBI raided Seidlitz' office at 300 N. Washington St., Alexandria, on Jan. 9, and recovered the computer printouts.

A second search warrant subsequently recovered the portable computer terminal and a diary that showed entries relating to the plan to steal the Wylbur program, Finney said.

Seidlitz, a mid-level executive who worked at OSI from Jan. 1 to June 17, 1975, was described at the trial by computer expert Robert Fitzgerald as "an extremely clever systems programmer" who is a highly qualified technician and mathematician.

Neeley said Seidlitz "technically resigned by mutual agreement" last summer. Before he left, according to Seidlitz' testimony, he frequently had complained about the lack of security on various U.S. projects there.

Finney, who was aided in the prosecution by Assistant U.S. Attorney Robert A. Rohrbaugh, said conviction of fraud by wire could result in fines of $1,000 and imprisonment for five years on each of two counts. Seidlitz will be sentenced after completion of a presentence investigation.

[From the New York Magazine, Aug. 2, 1976]

The Computer Did It

". . . COMPUTERS MAKE IDEAL ACCOMPLICES SINCE THEY KEEP QUIET, HAVE NO MORALS, AND CAN BE PROGRAMMED TO DESTROY EVIDENCE . . ."

(Books/Lori Andrews)

The 25-year-old supervisor of computer operations in a bank supplements his $13,000 salary with money from other people's accounts. He uses a utility program intended to change the content of any record in the system, then instructs the computer to destroy the evidence of his tampering. When a savings-account customer complains that his balance is $6,000 short, a computer shows nothing fishy. The overall savings-account balance is in order, since the $137,000 stolen from 25 customers has been transferred to the accounts of the culprit and his friends.

Computers—whether they monitor heart machines or record financial assets—create unique opportunities for crime. Donn Parker's

Crime by Computer (Charles Scribner's Sons, $10.95) explores the attraction of this modern form of social deviance with blow-by-blow accounts of the latest technological capers and prescriptions for computer safeguards. He concludes that businesses, governments, and institutions are rushing headlong into the cashless, checkless, and paperless society before considering the hazards associated with data assets. "We can't revert to previous methods; there is no pulling the plug on the machines." So the best Parker can do is warn users how and why the computer is compromised.

Parker has worked full-time since 1970 on the problem of computer abuse at the Stanford Research Institute. He characterizes computer crimes by the four roles computers can play:

The computer may be the *victim* of a crime motivated by personal, corporate, or political vengeance. Parker reports that in 1974 one programmer got so frustrated that he pulled out a pistol and shot his computer right between the bits. Also that year, the employee of a computer company broke into a rival computer service's facilities and set fire to the competitor's computer, peripheral equipment, and supplies. In 1970, political dissidents bombed a U.S. Army research-center computer. A common rationale in these cases is that "the victim deserved it."

A by-product of computer technology is the creation of a *unique environment* for new types of crimes. When a bank figures interest, it rounds its figures to the nearest penny. While it would not normally be worthwhile to rob an individual of a fraction of a penny, a programmer makes a hefty sum when he credits to his account the fractions rounded down from every customer's interest. Although technology creates new crimes, the law lags in determining how to deal with them.

The computer is the *instrument* of the crime when used as the perpetrator's tool. Parker recounts a newspaper report of the Senate Watergate Committee's investigation of a computer service secretly owned by a friend of Nixon's. The company, which was handling "McGovern for president" mailings, allegedly delayed the computerized mailing lists so that voters received the campaign literature the day after the election. Computers make ideal accomplices since they keep quiet, have no morals, and can be programmed to destroy incriminating evidence.

The use of computers as a *symbol* to intimidate, deceive, or defraud victims played a major role in the Equity Funding scandal. To inflate the value of its stock, Equity programmed its computer to show over $100 million in fictitious assets. Since computer data is assumed to be infallible, the fraud remained undetected for nearly a decade.

Three hundred and seventy-four cases of computer abuse have been reported in the past eighteen years. The computer criminals responsible were usually young, highly motivated, outwardly trustworthy, and had never been in trouble before. They were drawn to computer crime, says Parker, due to the "Robin Hood Syndrome": "believing that stealing from individuals is highly immoral but that stealing from an organization and in particular through a computer somehow does not hurt anyone.

"A computer is an ideal target for attack,'" explains Parker. "It can't cry, have its feelings hurt, get mad, or strike back. Yet, it has

certain personified characteristics that make it a highly attractive and satisfying target, and replaces the organization using it as the subject of attack."

The rationale that the computer "deserved it" inspires not only physical attacks on the symbol of a political ideology or a bureaucratic institution, but also crimes where the computer is used as a tool. Computer crime may be a way of getting back at automation which is viewed as threatening one's privacy or reducing one to a cipher.

An alternative computer-crime rationale, which Parker fails to explore, might be called the "We're Just Haggling Over the Price Syndrome." Like the woman in the joke who agrees to go to bed with a man when he offers her a million dollars, but is enraged when he suggests the same act for $20, a normally trustworthy person may become a computer criminal because the stakes are so high. One computer criminal told Parker that if he found a wallet with money in it, he would return it to its owner. But if he could steal $10,000 from an open cash register without detection, he would do so, as any "normal" person would.

The average "take" in a computer crime is $450,000. This tempting sum is hard to resist when a person realizes that detection is difficult and punishment is often slight. The volume of computer data makes it difficult to audit or inspect. And since many auditors lack computer skills, they often must rely on the potential criminal's aid. Even if a crime is detected, the company might not prosecute for fear that it would sustain a greater financial loss due to customer apprehension than from the crime itself.

In *Crime by Computer*, Parker's suggestions for reducing computer crime include encryption devices, ethics courses for computer users, and safeguards such as remote storage of copies of programs, limitation of usage of one's own data, and programs to report illegitimate use. As a computer technologist, Parker proposes safeguards which would alter the computer or its environment to achieve security. But his detailed technical solutions overlook the most difficult aspect of computer protection: selling it to computer owners.

The number of computers in use in the United States is expected to triple by 1980. But as long as a bank like Union Dime can recoup its embezzlement losses through insurance, or a company like Pacific Telephone can pass on the cost of computer-crime losses to its customers, owners of the expected 500,000 computers may not find computer security economically justified. And since insurance against computer abuse is now being offered, executives may have even less enthusiasm about instituting safeguards. Computer buyers do not want the added cost of computer security.

Meanwhile, assets and data about people continue to be compromised by computer abuse. The situation can only worsen as electronic funds transfer systems (EFTS) control a growing number of commercial activities. Both legislation and public clamor is necessary in order to convince computer users to implement Parker's well-thought-out proposals. Dr. John Weil, former director of engineering for a Massachusetts branch of Honeywell Information Systems, told Parker that providing secure computers is like trying to push on a string. The customer on the other end must be pulling to make it work.

[From the Washington Post, Aug. 1, 1976]

Convicted Computer Expert Seeks Role as Security Adviser

(By Bill Peterson)

A computer expert who was sentenced yesterday to three months in jail for using his skills to tap classified government computer files is now offering his services as a "security consultant" to government agencies and private companies.

Bertram E. Seidlitz, who operates a small computer firm in Alexandria and who was convicted of fraud in Baltimore's U.S. District Court, is circulating letters to potential clients who might need to protect their computer from people like him.

His services, the letter says, "would be made available at no charge."

The proposal, Maryland U.S. Attorney Jervis Finney said "seems highly questionable, highly doubtful to me."

Seidlitz admitted it took a certain chutzpah. He said his lawyer advised against it. "His advice was to sit back and hang my head in shame," he said. "But I don't operate that way."

So far Seidlitz has not had any takers. But he is keeping the offer open because he feels the problems of security in a computer age are too often ignored.

His case, which U.S. Attorney Finney has said "signals the future of white-collar crime," is a good one in point.

Using a computer terminal and a telephone as his burglary tools, Seidlitz tapped into a computer that contained classified files of the Federal Energy Administration, according to testimony in his trial.

Physically he did not go near the computer. He simply dialed the telephone number of the computer firm in Rockville where the FEA information was stored and punched secret passwords into a keyboard computer attached to his office phone. Over a period of 3½ months, he extracted 40 rolls of computer printouts.

Seidlitz, 38, of 8629 Brae Brooke Dr., Lanham, maintains he did it to show how lax security was at Optimum Services Inc. (OSI), where the FEA records were stored. He formerly worked as a mid-level executive at the firm.

But in sentencing Seidlitz in Baltimore yesterday, U.S. District Judge Alexander Harvey II noted that neither he nor the jury accepted this argument. A prison sentence, the judge declared, was needed "to deter others who, like (the defendant), would use their technical skills to steal from computers."

He also ordered 33 months probation for Seidlitz. He was convicted of two counts of wire fraud after an eight-day trial last June. Yesterday he and his attorney, Frank M. Kratovil, said they intend to appeal the ruling, which OSI president Stan Neeley has called a "landmark" in the computer industry.

The case, the first of its type in the Washington area, is one of a growing number involving computer fraud around the country. "This is the frontier of white-collar crime," prosecutor Finney said yesterday.

The same technique employed by Seidlitz could be used to gain access to other computers. Anyone with the technology and secret

access code numbers could tap into files belonging to his bank, the FBI, the Internal Revenue Service or other government agencies, Finney said.

Seidlitz said he had complained about the lack of security while employed at OSI, a complaint also voiced in a report a year ago by the General Accounting Office. He maintained the material had little value, except to prove his point.

During the trial, OSI president Neeley said the information Seidlitz obtained was valuable not because it divulged FEA secrets but because it would permit other firms to duplicate the complex system used to store FEA data. The system, he said gives OSI a competitive edge that has resulted in $30 million to $40 million in contracts.

The only reason Seidlitz was able to tap into the computer was because he was a former employee "who retained in his memory the keys to unlocking the information." Neeley said.

Seidlitz, who started tapping the computer Oct. 19, 1975, was first detected Dec. 30, 1975, when an OSI employee who was monitoring the computer noticed an unauthorized user on the line.

Company officials then contacted the C&P Telephone Co., which traced the call to Seidlitz's computer firm in Alexandria. The FBI raided his office at 300 N. Washington St. 10 days later.

[From Newsweek, Aug. 9, 1976]

The Computer Bandits

For Milo, a bright young computer programer with a habit of spending money he didn't have, things couldn't have worked out more conveniently. He had just been hired to computerize the check-handling system at the National City Bank of Minneapolis, the same bank where he kept his personal checking account. Milo diligently designed an elaborate program that would tell the bank's computer how to process checking transactions. But in the middle of the complex program, he slipped in an extra command of his own: the computer was instructed to ignore any of Milo's personal checks whenever his account didn't have sufficient funds. Milo got away with it for months, but then the computer broke down, forcing the bank to go back to processing checks by hand—and an ordinary clerk discovered the scheme.

Milo is just one of thousands practicing what U.S. attorney Terry Knoepp calls "the crime of the 1980s"—computer fraud. By using and abusing electronic brains, a new breed of white-collar criminal, skilled in the arcane lore of computer science, is costing banks, corporations and even the government uncounted millions in stolen goods, services and hard cash. Just how bad things have got is hard to say, since more than 85 per cent of all computer crimes may go undetected or unreported. In his recent book, "Crime by Computer," Stanford Research Institute's Donn B. Parker estimates the total take at about $300 million a year. That's small change compared to the $40 billion that was lost in 1974 from conventional fraud and embezzlement. Still, with more and more companies computerizing their operations—the U.S.

computer population is expected to grow from about 150,000 now to more than 500,000 by 1980—the potential for electronic fraud in enormous.

Struggle. As a result, computer manufacturers, auditors and lawmen are struggling to learn sophisticated ways to contain electronic breaking and entering. Just last week, a group of twenty Federal and state prosecutors met at the University of California campus in San Diego to study how computers work and to discuss methods of building better cases against electronic embezzlers.

It won't be easy. In part because people tend to accept any computer print-out as sacred truth, computer fraud is notoriously hard to detect if a criminal knows how to tell the computer to cover his tracks. A teller at New York's Union Dime Savings Bank, for example, embezzled $1.4 million over three years to pay his gambling debts—and was finally caught, not by the bank's auditors, but when police raided his bookmaker.

There are several basic ways to manipulate computers. Most simply, an embezzler who knows how to write a program can just tell the computer to do his bidding. A California accountant, for example, looted more than $1 million from his company by recording higher payments for raw materials in the company computer than the firm actually paid. He programed the computer to put the excess cash into the accounts of dummy companies he had set up—and also to advise him on how much money he could withdraw from those accounts without attracting notice. Only when he began making withdrawals at the rate of $250,000 a year was he found out.

Fake. A dishonest manager can also put false information into the computer's memory—as happened in the classic Equity Funding swindle in 1972. To pump up Equity stock, the insurance company's executives recorded the sale of 97,000 policies in their computer, when in fact they had sold fewer than 33,000.

A third form of computer crime involves plugging into a computer system by outsiders bent on "stealing" data. Last June, a former employee of the company that handles programing for the Federal Energy Administration was convicted of extracting the FEA's top-secret computer-operating program through a terminal attached to his telephone. With that program, the thief could have got access to much of the energy body's classified information.

Finally, the computer can be used to help crooks plan routine capers. Three years ago in Chicago, a ring of burglars recruited a computer to compile lists of prosperous targets, rather like an advertiser zeoring in on a rich market. With such electronic guidance, the gang stole more than $1 million in negotiable securities from private homes.

Since most computer frauds are perpetrated by "insiders," security specialists emphasize better screening of programmers and tighter controls on users. The computer itself is quite capable of repelling attempted "break-ins" by outsiders—but it is helpless when the passwords that allow legitimate users access to a system fall into the wrong hands.

International Business Machines Corp. has developed perhaps the world's most sophisticated computer security system to safeguard its own administrative network—which contains salesmen's orders, cus-

tomer lists and other valuable data. A fortnight ago IBM began selling a similar security system. As computer users tighten lax security, they may manage to curb the most obvious computer ripoffs. But as computers proliferate, so too will the number of well-trained crooks willing to match their wits with the computer.

ALLAN J. MAYER.

[From Time Magazine, Sept. 13, 1976]

INSIDE JOB

A standard complaint about prison rehabilitation programs is that they do not work. One such program at Leavenworth, the federal prison in Kansas, appears to have worked only too well. Six years ago, Leavenworth launched a computer training course under a federal contract. The computer course became so popular that 58 convicts are enrolled.

Small wonder. Inmates apparently learned how to crack the computer code governing Internal Revenue Service audits. Since prisoners must file tax returns on any outside income, some saw a golden opportunity. Knowing how to hoodwink the computer, they loaded their returns with all kinds of bogus claims for refunds, with little fear of being audited. One convict was finally caught. Last week he went on trial for receiving $20,000 in illegal refunds. Others are sure to follow him to the dock, since the total rip-off could range anywhere from $150,000 to $6 million. Back to making license plates.

[From the Privacy Journal, March 1975]

KEEPING YOUR BILLS SECRET IN AN ELECTRONIC AGE*

(By Paul Armer)

On the front page of *The New York Times* last year there appeared the expression "nutritionally endangered." Do you know what they couldn't bring themselves to say? "Starving."

Now, electronic funds transfer system (EFTS) is a high faluting way of describing a system that will replace money, check and credit card transactions (some, not all, the proponents will hasten to add) with a system that will eventually be on-line from the point of sale to your bank's computer. And when you make a purchase the amount of the sale will be debited to your account. (And thus the piece of plastic you use is called a debit card rather than a credit card.) Or you may elect to buy on credit, a distinction which isn't relevant to the primary question, since in both instances the information about the sale reaches the computer in real time and is recorded. (Experts guess that there are now about 300 billion transactions in cash per year; about 75 percent for less than $1, and only 5 percent exceeding $10.)

Checks are involved in a transaction only about a tenth as often as cash; 90 percent are for greater than $10. And one percent are greater

*Adapted from remarks at the last national conference of the Association for Computing Machinery by Paul Armer, coordinator for the program on technology and society, Center for Advanced Study in the Behavioral Sciences, Stanford, Calif.

than $10,000 but account for 80 percent of the dollar value. It costs roughly 20¢ to process a check, making a rounded total cost of our demand deposit accounting on the order of $10 billion. The number of checks has been growing at about 7 percent per year.

In summary, cash transactions represent about 90 percent of the total, but, of the transactions over $10, only about one-third are for cash.

There are two nationwide bank credit card systems—BankAmericard and Interbank Master Charge. Each has an electronic nationwide credit authorization system. National BankAmericard (NBI) has brought up a system to handle interbank transfers electronically. Thus, if you make a charge today with your BankAmericard and the merchant gets the chit to his bank today, later tonight that transaction will be in the records of your bank. And the cost is 2.5¢. That means that country club billing (you get a copy of the receipt you signed in the store) is a thing of the past, although some banks will print facsimiles to try to keep you happy. Descriptive billing is what most of us will be forced to accept.

Both BankAmericard and Master Charge are busily designing systems that will connect, electronically, point-of-sale recorders in a store and remote bank teller machines to your bank's computer, debiting the sale amount to your account (or recording it for future debiting) all in real time. Implementation will begin this year.

There now exist four so-called automated clearinghouses which support the automatic deposit of payroll checks and automatic preauthorized payment of fixed monthly debts, like mortgage or car payments. Some of them also provide a service called "bill check." Here, for example, the local utility sends you a bill, part of which is a check which you sign and return to the utility. They batch the bill checks and transmit the data, not the checks, to the local automated clearinghouse, which debits your bank which then debits your account. This is not now on-line, but like the present systems of the bank credit card companies, could be upgraded.

This procedure is not now heavily used although Equitable Life Assurance Society, working with Chase Manhattan Bank, has its monthly transaction volume of preauthorized payments up to about 100,000. The thrift institutions are moving rapidly in implementing EFTS systems. MINTS (Mutual Institutions National Transfer Systems, Inc.) permits its card holders to do any banking business they might do at their home bank at any other MINTS member bank. MINTS' avowed hope is eventually to tie this service into a national network "hopefully managed by the Federal Reserve Board." One almost gets the impression that the commercial banks and the bank credit card systems are racing towards implementation of true real-time EFTS to get there before the thrift institutions and the Federal Reserve Board. Of course they're also much interested in the cost savings this will bring them.

And what is the Federal Reserve System doing? For some time all checks in excess of $10,000 have been cleared electronically over "Fed wire." Remember that such checks are 1 percent of the total number but represent 80 percent of the dollar volume. Since 1947 the proportion of total deposits under the direct control of the Federal

Reserve System has dropped from 86 to 77 percent and the pace of dropouts has been increasing. So the Federal Reserve System aspires, in my belief, to have "a" (and preferably "the") EFTS, which every bank would have to use. And, in order to use it, each bank would have to be a member of the Federal Reserve System. The Fed published a proposal to expand the Board's Regulation J, which governs the use of the Fed's facilities to collect checks, so as to permit the electronic transfer of funds. (38 Fed. Reg. 32952, Nov. 15, 1973, proposed 12 CFR 210.) The Fed solicited comments on the proposed changes, but mentioned only economic and financial implications. In 37 pages of material nothing was said about social implications—the word privacy does not appear. Little was said about security and access.

They received over 200 responses. They've been silent ever since. They give the impression that they'd prefer it if we'd leave them alone and cease saying there may be some social implications.

But while silent they haven't been inactive. The Fed, the Treasury and the Social Security Administration have begun depositing Social Security checks directly into the recipient's bank account in Georgia through the local automated clearinghouse. Florida recipients will be added in April and by 1976 the scheme will be implemented nationwide. The Treasury wants to cease entirely writing checks for routine periodic purposes.

The National Science Foundation has given a grant to Arthur D. Little, Inc., to do an assessment of "Less Cash/Less Check Technology." They published a first phase report in February 1974 and said on page 101: "In latter phases we will investigate how deep and how broad the concern for privacy is and how it will impede change in the payments system."

My god—that's like being concerned only over the public's opinion of whether smoking is dangerous to one's health and how that concern will impede the sale of cigarettes. Investigation of whether or not EFTS represents a threat to privacy seems not to be a question to be addressed!

One expert predicts that by 1980 one-third of all purchases would utilize the bank debit card system, replacing about 70 percent of check utilization in the process.

The important variables to me are whether the transaction from beginning until it reaches my bank is on-line or not and what percentage of the transactions, particularly those more than $10, are other than cash. The extreme case, in which all transactions go through the system in real time, obviously represents the greatest threat to privacy. It is unlikely that we'll get to the extreme case in the near future, if ever.

Several years ago I was a member of a team which was given the assignment of assuming that we were data processing advisors to the Russian Secret Police (the KGB) and then designing a system for maintaining surveillance of all Soviet citizens and foreigners within the USSR boundaries. After some study, we decided that the easiest and cheapest way to do it was to install a real-time EFTS which would handle all financial transactions. You see, such a system knows where an individual is in real time, as well as what he is buying, every time he makes a financial transaction. A system that knows

where each individual is represents a great surveillance system for would-be tyrants. You can't alleviate my misgivings with legislation against using the system in that fashion since, in one of my scenarios, there has been a take-over of the government and all civil liberties suspended in the national interest. Legislation would be meaningless.

But much less extreme cases disturb me. In our existing payments systems, privacy is assured under all but the most unusual circumstances by the sheer cost and inconvenience of a manual search. EFTS, even non-real-time EFTS, would concentrate an enormous amount of financial information about an individual in one place—intimate details of his personal life.

[From the Washington Post, Feb. 26, 1976]

Fed Keeps Hillside Vault

BILLIONS IN BILLS HELD IN CASE OF ATOMIC WAR

(By Charles R. Babcock)

Culpeper, Va., Feb. 25.—In what could be called the Ft. Knox of paper money, the Federal Reserve Board has stockpiled billions of dollars in cash in a heavily guarded, little-known complex carved into a hillside near here.

The huge supply of new bills—believed to be the most kept in any vault in the world—would be used to replenish the nation's money supply in case of a nuclear attack.

Federal Reserve officials are reluctant to talk about the value of the 700 million "notes" stored in the Culpeper facility, about 80 miles southwest of Washington.

But from rough calculations it can be estimated that the cache of unused currency—in denominations from $1 to $100—totals several billion dollars.

The bunker-like facility also houses a records center and a sophisticated computer operation that currently directs communications among the 5,700 member banks of the Federal Reserve system.

The seven-member Federal Reserve Board controls the basic money supply by buying or selling government securities, among other means.

Culpeper is the most elaborate of a series of "relocation centers" set up by The Fed's 12 district banks as part of the nation's emergency preparedness plan.

The center, built in the late 1960's was designed to be the new home of the Richmond district bank—and apparently the Board itself—after a nuclear war.

About 100 persons work there full-time—about 30 in administration and records, 30 in the computer operation and about 40 in security.

The security force is supplemented by an elaborate system of television surveillance.

The center is located inside Mt. Pony, just off U.S. 3 near Culpeper, a town of 7,000 in the foothills of the Blue Ridge Mountains.

It was built to withstand both blast and radiation from a nuclear attack.

Space for the three-story 400-foot-long structure, which slopes back with the hillside, was blasted out of solid rock. Gordon Grimwood, the Fed's top emergency planning officer, said in a recent interview: "We dug a hole in the side of the mountain, built it, and covered it up again."

Two to four feet of dirt covers the foot-thick concrete walls of the building. Lead shields are positioned to be raised over windows in case of attack.

The facility also has its own water, air filtration and power facilities, and enough freeze-dried food to last 30 days.

In addition, there is office and dormitory space for the families of the Fed officials on "the list" of those to be relocated there.

On the second floor, plastic covered desks and chairs sit at the ready in empty offices. On the third floor, there are 200 empty bunk beds.

"We can sleep 400 people here by using a hot bed system (sleeping in shifts)," Grimwood said.

Though Grimwood declined to confirm it, there are strong indications that the Culpeper center also would be the new headquarters for the Federal Reserve Board itself in case of attack.

Other emergency centers for the district banks include a limestone mine in western Pennsylvania, the bottom of a salt mine in Kansas, an abandoned communications bunker at a military air base in Massachusetts, and basement rooms on several college campuses across the country. Most are merely depositories for bank records.

The existence of the Culpeper facility as a communications center is well-known in the banking community. It is referred to as "the fed wire" or the "Culpeper switch."

But the details of the center's function in storing the nation's emergency money supply is not widely known.

Congressional banking committee staff members expressed surprise at the complicated hardware housed in what one called "the hill with windows."

Most of the townspeople have heard only rumors that the facility is used to store money. J. B. Carpenter, Culpeper's mayor—and manager of Central Hardware—recalls, in fact, that when the center was being built people were told specifically that no money would be stored there.

Al Tinkelenberg, a vice president of the Fed's Richmond district bank and head of the Culpeper center, confirmed that an early decision was, "let's just not tell people about the money."

But during a dedication speech at the center on Dec. 10, 1969, then Federal Reserve Governor J. L. Robertson "spilled the beans," Tinkelenberg said, by referring in some detail to the cash reserve.

A Federal Reserve brochure about the "Culpeper switch" computer operation makes no reference at all to the center's "other" mission.

"Obviously, we'd rather not talk about how much money is stored here," Tinkelenberg said during a tour of the facility earlier this week. He and Grimwood both refused to put a value on the cash in the massive vault at Culpeper.

But a review of annual Fed reports to the Joint Committee on Defense Production shows that in past years as many as 1.9 billion "notes" have been stockpiled throughout the Federal Reserve system and even in some commercial banks.

The original goal, according to the reports, was to set aside a two-year supply of currency. This was based on the assumption that the Bureau of Engraving and Printing would be knocked out in an attack and would not be operational again for two years.

But by 1973, the annual issue of notes had grown so large, that the Fed "retreated," in Grimwood's words, to basing its emergency needs on the excess of note issues over redemptions for the most recent two-year period.

Thus, the most recent report for fiscal year 1975 shows an objective of 500 million "notes." That is, there were half a billion more notes issued than redeemed in 1973 and 1974.

Right now, the Culpeper vault holds 700 million notes. "We do have a cushion," Grimwood said.

Several sources familiar with the center have said those notes are worth "several billion" dollars.

Assuming the same mix of different denominations as the Bureau of Engraving and Printing uses—printing more than 50 percent in $1s, 15 percent $20s, 10 percent $5s and $10s and less than 1 percent in $50s and $100s—the value of the notes in Culpeper would be at least $4 billion.

Beyond the magnitude of the money involved, the story of the Fed's emergency center at Culpeper tells something about the state of the nation's "doomsday" planning.

It is a story that involves talk of "kill ratios" and "radiation decay equations" and "attack patterns." Gordon Grimwood has been living with such end-of-the-world scenarios for 20 years now.

"I recognize that this is a topic people don't like to think about," he said in a recent interview. "The attitude seems to be, first, 'It can't happen.' And then, 'If it does happen, there won't be anyone left anyway.'

"I certainly can't guarantee that our plans will work, but without them—if there is a nuclear war—everyone will take to the hills. We'll be back to tribal warfare and there'll be no hope for national survival and recovery," Grimwood said.

The Fed's emergency plan, like those of all other federal government agencies are predicated on assumptions that there will be people left to use bank and otherwise carry on life.

Daniel J. Cronin, assistant director for conflict preparedness at the Federal Preparedness Agency, said yesterday that computer war-games by his agency predict that half the American population would survive even an all-out nuclear attack.

Large parts of the country would be left relatively undamaged, he added. Furthermore, the latest strategies of world powers lean toward the capability or possibility of limited nuclear strikes, Cronin said.

"So we're really not talking about the end of the world," he said.

Cronin added that the Federal Reserve Board has been a leader in emergency preparedness planning. Its mission, under an executive order signed by President Nixon in 1969, is to restore the nation's banking system—including the money supply—after an attack.

Emergency planners say their most difficult mission today is convincing agencies of the need to keep their readiness current.

For instance, in a report to Congress on the lack of preparedness by small commercial banks, the Fed has said repeatedly that a major prob-

lem is "a tendency to let preparedness activities drag during periods of quiescence in international tensions."

The same attitude has been expressed more recently by Grimwood's boss, Federal Reserve Board Chairman Arthur Burns.

In 1973, he asked the President's Office of Management and Budget to review the assumptions "underlying post-attack financial policies . . . in the light of the current military and political environment."

That review has yet to be completed. But in the meantime, the Fed's efforts to upgrade its district bank relocation centers has been halted, Grimwood said. "There have been no new initiatives," he said.

Still the Federal Reserve is considered almost in a league by itself when it comes to emergency planning.

For one thing, it and the Treasury Department are the only agencies that have made plans for housing the dependents of its selected relocation officials.

One reason for this may be because the Federal Reserve is one of the few agencies that don't come under the congressional appropriations process.

Rep. Wright Patman (D-Tex.), a longtime foe of the Fed's independent spending habits and chairman of the Joint Committee on Defense Production, said through an aide yesterday that he wanted to know more about the Culpeper center and its functions.

The Fed's annual preparedness reports to Congress have been similar to the agency's other responses to legislative overseers, he said, "traditionally evasive, reluctant and incomplete."

The reports to the joint committee, for instance, give no indication of the costs of the Culpeper facility, he noted.

But until last year, a study of the reports shows, it doesn't appear that anyone ever asked.

William Kincade, staff director of the committee, said yesterday, in response to a reporter's question, that the committee now plans to ask.

[From the Washington Post, Feb. 26, 1976]

Funds Switched at Culpeper

Unlike the closely held knowledge that its Culpeper, Va. facility holds billions of dollars in cash, the Federal Reserve system freely hands out a brochure about "The Culpeper Switch," the elaborate computerized communications operation located in the same fortified building.

The illustrated, 20-page color booklet tells how, as a free service to its member banks, the Fed has set up a multimillion-dollar network to insure nearly instantaneous relay of money transfers all across the country.

The "switch" is designed to process 25,000 messages an hour through four large computers, which cost nearly $3 million to buy and install in 1968. The operating budget for 1975, including maintenance and salaries of the 30 technicians, was nearly $650,000, a cost shared by the 12 districts.

Most of the traffic is wire transfers—that is transfers of money from one account to another in different parts of the country.

For instance, when a corporate customer of a bank in New York wants to shift money to a company account on the West Coast, his bank requests the transfer through the Fed's New York district bank.

The message is then relayed through Culpeper's computers to the nearest district bank on the West Coast and then on to the customer's personal bank. The whole process takes just a few minutes.

Al Tinkelenberg, a vice president of the Richmond district bank and director of the "Culpeper switch," said during a recent tour of the facility that elaborate precautions have been taken to prevent someone from tapping into the computer system and fraudulently siphoning off funds into a phony corporate or personal account.

He noted that the system has back-ups in case of technical failure and even has its own battery power supply which compensates for slight fluctuations in the commercial power.

Because of the increasing volume of traffic on what bankers know as "the fed wire," there is a charge of $1.50 for every transfer of less than $1,000. "We want to have the vital few instead of the trivial many," Tinkelenberg said. "Otherwise the volumes would kill us."

The large, so-called "money center" banks in New York and Chicago make the most use of the switching facility, he added.

Doesn't this amount to a taxpayer subsidy for these financial giants? "Yes, it is a nice thing for the banks," Tinkelenberg said. But he added that small banks can use the free service, too.

There has been discussion for some time about charging all the users of the switch for the service, a Fed spokesman said in answer to a reporter's query. No final decision has been made, he said.

CHARLES R. BABCOCK.

[From the New York Times, Apr. 11, 1976]

FUND PLAN CALLED PERIL TO PRIVACY

WHITE HOUSE AIDE SCORES PROPOSED CLEARING CENTER FOR FINANCIAL TRANSACTIONS

(By David Burnham)

WASHINGTON, April 10.—The White House Office of Telecommunications Policy has charged that a plan to build a national center for the electronic transfer of funds could give the Federal Government "a highly effective tool for keeping track of people and enforcing 'correct' behavior."

The criticism was directed at changes proposed by the Federal Reserve System that would enable its existing computers to operate a national clearing center for financial transactions recorded as electronic impulses, as well as those recorded on checks, deposit slips and other paper.

Americans, through the use of credit cards and automated teller stations and other credit systems, are increasingly completing their transactions through electronic impulses rather than through cash or checks.

The criticism of the Federal Reserve System proposal was made by John Eger, acting director of the White House Office of Telecommunications Policy, in a brief filed with the system on April 2.

COMPUTERS AND TELECOMMUNICATIONS

Mr. Eger said that electronic funds transfer was the product of an interconnection of computers with telecommunications.

"On its simplest level, what has been created is the ability to directly interconnect the records which indicate the availability and transferability of funds in an individual's account," he said.

"There is a danger that government operation [of a monitoring system] may ultimately pose very real threats to the privacy of individual citizens," he continued. "A detailed monitoring of the information carried on such a system could easily generate data on a user's buying habits, political activities, physical movements and so forth."

Mr. Eger noted that the Internal Revenue Service, while initially created as an independent agency with the sole function of collecting taxes, has become "a repository in which other agencies of the Federal Government seek weapons for criminal prosecution, as in the case of the Justice Department, or, as we have seen in recent years, even for political harassment."

The official thus predicted that, if the Federal Reserve Board should move ahead with its central switching computer, it would come under increasing pressure to divulge details about the finances of individuals.

REQUEST FOR COMMENT

Mr. Eger's criticism was made in response to the Federal Reserve System's request for comment by other agencies and interested parties. Joseph R. Coyne, a spokesman for the reserve system, said today that its board of governors had not yet formally considered the comments submitted, although they were being studied by the staff.

Furthermore, Mr. Coyne said, assurance has been given the National Commission on Electronic Funds Transfer that no final action by the board of governors would be taken on the proposal until the commission had had an opportunity to submit its comments.

The commission was created by Congress in October 1974 to inquire into what kind of electronic funds transfer system should be set up, who should own it, how it should be financed and who should have access to the information.

President Ford did not name the commission members until last October, and the commission held its first meeting on Feb. 6.

F.B.I. PLAN BLOCKED

Last year, Mr. Eger voiced strong opposition to a Federal Bureau of Investigation plan to operate a central switching center to help the states exchange criminal justice information. His complaints that such a system could lead to centralized police enforcement in the United States were an element in Attorney General Edward H. Levi's decision to block the F.B.I. proposal until Congress passed legislation dealing with the problem.

The Federal Reserve System plan has drawn mixed reaction from the financial community. The larger banks generally oppose it because they want to operate, or join, private switching networks. On the other hand, such groups as the National Association of Mutual Savings Banks have applauded the proposal.

In addition to criticizing the Federal Reserve System proposal because of its potential threat to individual privacy, Mr. Eger said that it would tend to block the entry of private companies into the electronic funds-clearing business.

In addition to commenting to the Federal Reserve System, the Office of Telecommunications Policy is working on amendments to the Federal law restricting official eavesdropping. One aspect the office is examining involves the law's restriction only to the eavesdropping of oral communications and not the secret recording of written transmissions.

[From the New York Times, Aug. 1, 1976]

There Was Once Money. Wasn't There?

(By David B. Saxe and Dorothy F. Pariser*)

The largely unheralded development of Electronic Funds Transfer Systems is moving a credit-card-conditioned society toward a completely cashless environment, with severe repercussions for the American consumer.

The systems accomplish the electronic transfer of funds from one person's or company's bank account to that of another, providing a completely integrated computerized financial system through which the intermediate steps of paying numerous bills and charges by cash or check would be eliminated.

Thus, John Doe enters a supermarket, collects his groceries, inserts his personal plastic EFTS card at the checkout register and, after authorizing $100, automatically pays $19.93 for his purchase and receives $80.07 in change. He then returns home, inserts the same card into a slot in his telephone, dials a series of encoded numbers, and pays his rent and utility bills. Restaurant bills and theater tickets are similarly handled.

The system is activated by Mr. Doe's EFTS credit card, which instructs a master computer to debit his account by the amount he spends or specifies, and to credit simultaneously the account of the establishment providing the services or goods.

Embryonic systems now exist in some banks. In certain retail establishments with point-of-sale terminals, at the time of purchase the credit of the individual can now be verified, his account charged and the sale totaled by means of a computer.

An advanced system would appeal to the consumer because of its convenience. The need to carry cash, the often burdensome task of writing checks, and the need for mailing bills would be eliminated.

EFTS has the potential of offering dollar savings to the consumer. Computerized computations should improve the accuracy of billing and payment systems, and the consumer will have direct computer access to his bank account at any time. The payment of stated, periodic charges can also be handled automatically. Through its automatic verification system, EFTS will eliminate bad checks, bank overdrafts, and failure to pay reoccurring fixed expenses when due.

---

*David B. Saxe is consumer advocate for New York City and director of law enforcement of the Department of Consumer Affairs. Dorothy F. Pariser, a consultant on advanced technology, is doing research on electronic transfers systems.

Nevertheless, this system may present serious drawbacks to the consumer. EFTS will take away much of the consumer's active control of his finances. If at any time his bank balance is insufficient to cover the payment of fixed, programed bills, he would no longer be able to decide which to pay first; the computer would make this decision for him. Also lost would be the grace period intrinsic to the current checking system, which helps consumers to "float" large expenses.

An even harsher blow to the consumer would be his inability to stop payment of a check if the purchased goods were defective or the services rendered unsatisfactory, a powerful weapon available to him against unscrupulous businessmen.

Accordingly, some mechanism must be built into EFTS to permit consumers to retrieve a completed transfer within a reasonable time.

Furthermore, tangential problems might arise. No longer would a periodic, easily understandable statement be sent to the consumer enabling him to maintain accurate control over his banking transactions. With no canceled checks, what legal proof of payment would the consumer be able to offer?

The centralization of the financial transactions of a consumer in the EFTS also poses enormous problems in the area of consumer fraud.

A felon operating in an EFTS environment could manipulate the accounts of the master computer and credit his own account with limitless funds. Although voice prints or fingerprints may be able to thwart such attempts, these security devices might make the whole system prohibitively expensive.

The most ominous drawback of EFTS for the consumer is the potential for invasion and loss of privacy. Every transaction that an individual makes would be centrally recorded, thereby permitting a complete profile of an individual's spending habits and whereabouts. Legislation would be needed to control the type of information collected and to regulate its dissemination.

The growth of EFTS is inevitable. Yet no consumer groups have taken positions to insure the integrity of consumer rights as EFTS progresses. In fact, these groups appear to be largely unaware of the system's evolution.

Consumers must be informed that while an Electronic Funds Transfer System offers many practical benefits, it could portend the early arrival of an Orwellian society if not properly regulated.

[From the Washington Star]

ELECTRONIC FUNDS TRANSFER SYSTEMS RAISE THORNY ISSUES

'BANKTAPPING' LOOMS AS REAL THREAT TO PRIVACY, MATHIAS SAYS

(By John Holusha)

This summer the House Banking Committee let loose a blast at the Treasury Department. Hundreds of Social Security recipients had written to complain that banks were failing to notify them that their checks had been deposited.

Some even said checks they wrote bounced after the directly-deposited funds were supposedly in their account.

Banking Committee Chairman Henry Reuss charged that banks were abusing the new system simply to save postage costs.

The confusion and anger over the program to eliminate the mailing of paper checks could be just a hint of what's in store for consumers as the nation moves inexorably toward greater use of paperless payments—the so-called electronic funds transfer systems.

This and other, less obvious, potential problems are currently being studied by the National Commission on Electronic Funds Transfer—established by Congress when it found itself confronted with the onset of EFT technology.

The 26-member commission has reached few conclusions—except to disagree with some courts over whether a remote terminal is the same as a branch. Internal staff papers, however, outline the scope of the issues to be addressed.

One of the thorniest is privacy. One commission document quotes Justice William O. Douglas on the issue of access to financial records:

"In a sense, a person is defined by the checks he writes. By examining them, the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads and so on ad infinitum."

The government has the right now to seize anyone's financial records, but a certain amount of effort is involved and records would have to be brought together from different places.

In a well developed EFT system all these transactions would take place electronically and records would be in computer data banks. A government investigator—or an eager aide compiling "enemies lists"—could theoretically punch a few buttons and call up a vast trove of information on any individual.

Maryland Sen. Charles Mathias has commented that government "banktapping" has become "a very real threat to the freedom and privacy of every American."

"The EFT world is a world of cheap, easily accessible data," agrees commission executive director Dr. John Benton. "The question of what information the government should have is a public policy decision that should be made openly."

Linked to the privacy issue is the one of how much role the government will have in EFT. Right now the Federal Reserve System operates the "Fed wire" which assists in intercity clearing of checks. It is planning to test a system linking automated clearing houses in six cities.

The commission has developed a leery attitude toward having a government agency positioning itself in the middle of the payments system. The key position is the transfer of payment from buyer to seller at the point of sale—the "POS switch" in EFT jargon.

"If the government runs POS switches the potential for abuse is clearly there," Benton comments. "The cost of obtaining information would be low and there would be ease of access."

As one of the commission documents notes in a burst of bureaucratic candor:

"Once the ability to gather, store, sort and file a variety of different kinds of data exists, most organizations tend to follow a Parkinson's Law that the data expand to fill the capability available to process it."

Less serious, but potentially more irritating to consumers is the question of what to do about "float."

Float is the time between when a person writes a check or signs a credit card slip and when the funds are actually deducted from his bank account.

Almost everyone has played the float at one time or another. The most common example is writing a check for more than there is in the account and then rushing to the bank to make a deposit. More sophisticated persons deliberately use a credit card for purchases in order to get up to two months free use of someone else's money.

As the commission's staff notes, float is a big item nationally, as much as $40 billion. In an EFT system, with almost instantaneous payment, this float would disappear unless deliberately designed in.

Without this, all a person's bills would come due at once as he was hooked into the EFT system and the float was squeezed out. "Consumers in the aggregate would pay an extremely high price at that time," the document says.

A related problem is the loss of consumer bargaining power. Without float there's no stopping payment on a check if a customer feels he's been taken.

The commission is due to file its report next year and has to come up with recommendations on the rights of consumers confronting EFT systems (as well as equally thorny inter-industry questions).

Surprisingly, even in the area of privacy there is little agreement. Some argue that strict privacy protection is not in the consumer interest.

"They argue that consumers have given up certain rights of privacy in order to achieve some of the efficiencies and cost reductions that can accrue from large-scale computer systems. Accepting the benefits of such computerization, the consumer has traded away some rights of privacy," the staff study says.

The commission will hold public hearings in Washington on consumer issues on Oct. 27 and 28. Subsequent hearings will be held on industry issues. An interim report is due in February.

[From the New York Times, Aug. 4, 1973]

TV System Aids School Security

This day in "Futuresville" a young woman stalls a hold-up man, confident that help is on the way—even though she hasn't screamed or pulled a police alarm, United Press International reports.

That same way in "Futuresville" an elderly man falls to the sidewalk. Before he passes out from one of his periodic heart spells, he knows help is on the way. But like the young woman in distress, he didn't scream for help or phone for it.

All over town that day as any day in "Futuresville" people in various states of distress, like the young woman and elderly man, summon help by pressing a button on a signalling device that looks like a ballpoint pen.

The citizens of "Futuresville" had been issued the ultrasonic device in connection with a security system. Pressing the button sends a silent

signal to a receiver in the police station. The system is so sophisticated that the police know at once exactly where to send help.

The technology involved in the system was from the National Aeronautics and Space Administration. Signalling devices of the type used in the "Futuresville" security system had been developed for the space program.

Some earthlings don't need to wait for the emergence of "Futuresville" to take advantage of the development. Such a system is helping teachers summon help when things get unruly in their classrooms or school corridors.

Six schools in Georgia, the Sacramento, Calif., high school, and two schools in New York City have such a system. The teachers wear the small, pen-size ultrasonic devices in a pocket. The push of a pen button lights up on a grid in the security office, showing the teacher's location. Help is dispatched at once. The teacher knows help is on the way because the pen signal also lights up a small square green panel in the hall or in her classroom. When that light goes out it means "signal received and help is en route."

The present and future use of the signalling device was described in an interview with Norman Schlaff, president of Norcon Electronics Inc., a New York communication firm.

He said a block association in New York is investigating installation of such a system for its members. A person needing help inside a house, for example, would press his pen button and a light would go on either outside his house or apartment. And a noise-maker would be activated, too, attracting further attention.

Mr. Schlaff sees a use for the devices in apartment corridors—especially as signaling systems for persons who live alone and get into stressful situations.

BRAWNY TEACHERS USED

In the schools, he said, most often a brawny faculty member is sent on the rescue mission.

"Usually, it it is a phys-ed teacher," he said.

Mr. Schlaff's firm also has installed closed-circuit television in two schools in Brooklyn.

Sponsored by the East Flatbush Neighborhood Action Program, the system cost $34,000 and has a control unit consisting of nine monitors located in the dean's office that "watches" the activity through cameras.

The cameras are situated at all entrances, in the corridors, and in the cafeterias. The main screen in the dean's office can be switched from channel to channel, picking up the view from the other cameras. In addition, every area has an intercom so an official of the school can speak to a student or an intruder.

[From Newsweek Magazine, March 10, 1975]

Bugging School

To passers-by, the two-story concrete-and-glass building, fringed by palm trees and a neatly landscaped lawn, seems no different from

scores of other private business facilities in Fort Lauderdale. But once inside, visitors are immediately confronted by a blunt sign on the receptionist's desk. It reads: "U.S. Government regulations prohibit any discussion of this organization or this facility. Sorry, the receptionist is instructed not to answer related inquiries."

The subject of these strictures is a professedly private school called the National Intelligence Academy (NIA), and its avowed function is to teach advanced electronic-surveillance techniques to qualified police officers and other law officials, in or out of uniform. Just why the receptionist's sign tries to invoke the authority of the U.S. Government is but one of a number of puzzlements about the place—particularly since everyone from NIA director Ronald Stanley on down is emphatic in denying that the outfit has any connection, financial or otherwise, with Washington. Stanley himself sloughs off most inquiries. "We'd just as soon that articles about us never appear, he says, "but we can live with it."

In the past sixteen months, the NIA has taught the sophisticated skills of electronic spying to police officers—many of them undercover agents—from 25 states and at least two foreign nations. In a grueling two-week course, the lawmen learn about magnetic tape, transmitters and receivers. They study the use of "body bugs" and the many applications of night-vision devices. They learn how to adjust an antenna so that intervening buildings don't blur their listening devices and how long a battery will last under varying weather conditions. They are given five minutes to bug a room secretly—while instructors monitor them by closed-circuit television.

Boost. Except for the $760 tuition paid by the students' sponsors, no government funds support this unique program—at least so far as anyone knows. The NIA's financial backing comes from a nonprofit foundation controlled by Leo Goodwin, 57, the multimillionaire heir to an enormous insurance company fortune. A former Army parachute instructor who shuffles around his 25-room Fort Lauderdale mansion in slippers to ease the strain on his jump-scarred feet, Goodwin is a cop buff who recently told an interviewer: "The whole country is on the verge of anarchy . . . I just felt that law enforcement needed a boost and I am doing what I can in my own small way to assist them."

Goodwin's assistance has amounted to at least $3 million over a three-year period for a school whose annual operating budget is estimated at one-sixth that amount. A million-dollar beachfront hotel was purchased to accommodate the visiting police students. Goodwin's foundation has also paid for NIA's headquarters, which will include a 20 by 12-foot miniature city, complete with buildings, trees, cars and people, so that surveillance tactics and techniques can be demonstrated in three-dimensional fashion. The building is equipped with all the latest gadgetry in electronic spying equipment—most of which happens to be manufactured by an outfit called Audio Intelligence Devices (AID), a company that has its own headquarters in the same building with NIA.

AID is owned by an interesting figure named Jack Holcomb. NIA director Stanley denies any financial ties between the nonprofit academy and the manufacturer, but the police students are regularly offered tours of the AID plant, and since the police learn electronic

surveillance almost exclusively with AID equipment, many of them may buy it for their departments when they go home.

Intrigue. Despite these disavowals, AID president Holcomb does serve the NIA as a "special consultant." Holcomb, 47, chews through 25 cigars a day and seems to keep two secretaries and an electronic paper shredder busy throughout his working hours. He was once thrown out of Anguilla by British officials who accused him of nefarious business dealings with rebel authorities. He was later asked to leave Haiti by authorities who accused him of being a U.S. agent. "Intrigue gets in your bloodstream like a narcotic," says Holcomb. "Once you get a taste of it, you want more." Holcomb has been variously allied with U.S. law and against it. He has publicly boasted of being contacted by the FBI to handle "anything the Feds wouldn't touch." His record shows three arrests, for barbiturate possession (charge dropped), wiretapping (acquittal) and nonsupport of a minor child (conviction). He now pays support but denies the child is his.

Holcomb and Goodwin apparently first met in the 1960s, and their relationship blossomed quickly. Holcomb advised Goodwin on the organization of NIA in 1972, beginning with a staff of veteran government investigators, including an old hand from the Central Intelligence Agency. Recently, many original instructors left NIA in a cross fire of recrimination. They accused Holcomb of using the school to boost AID sales; he accused them of planning courses on such illegal tactics as lock-picking.

Suspicious of Holcomb's foreign experiences, some people are now hinting that the NIA may actually be designed to provide international security training on behalf of the CIA, a charge that both director Stanley and U.S. Government officials regularly deny. So far, the only foreign police known to have trained at NIA have come from Canada and Venezuela. But Stanley reports with some pride that six foreign nations have inquired about enrolling their police and that on one occasion, a group of touring foreign dignitaries was escorted to the school by Secret Service agents.

Skills. Many graduates have high praise for NIA. Sgt. Lenny Angello, technical chief of the sheriff's organized-crime unit in Reno, Nev., calls NIA "the finest school of its type I have ever attended." Stanley contends that it fills a specialized need in law enforcement, much like the Traffic Institute at Northwestern University. "If a police officer is trained in surveillance skills," he says, "he is not only less likely to make a mistake, but less likely to abuse the law." The first subject in NIA's curriculum, in fact, is a thorough look at wiretap regulations, and the continuing theme of the whole course is how to bug citizens without violating the law.

—Jerrold K. Footlick with William Schmidt in Fort Lauderdale.

[From the Washington Star, Mar. 25, 1976]

Keep Technology for Friends, Pentagon Panel Says

(By Henry S. Bradsher)

A Pentagon task force has recommended that the transfer abroad of revolutionary advances in technology be permitted only to allied coun-

tries, provoking complaints from some U.S. industries that they might lose Third World markets.

The task force of the Defense Science Board studied prevention of transfer of militarily useful technology, industrial equipment and products to Communist countries. It proposed some loosening of present restrictions, shifting emphasis from limiting sales of equipment and products to controlling design and manufacturing know-how.

"Control of design and manufacturing know-how is absolutely vital to the maintenance of U.S. technological superiority" in strategic fields, the task force felt.

It sought to prevent "leakage" of major new technologies through neutral countries to potential enemies, as has been occurring, by applying the limits on Communist trade to all nations outside the present Western control system.

The Defense Department is now studying the task force's recommendations, which would require extensive changes in the present system of controlling foreign trade. The department plays a key role in the system in combination with the State and Commerce departments.

Although Principal Deputy Secretary of Defense William P. Clements Jr. has ordered that an implementing plan be developed, a Pentagon spokesman said yesterday the department would not necessarily push all the recommendations.

When the task force report was made public Tuesday at a hearing of the Senate Banking Committee's international finance subcommittee, representatives of electronics, computer and machine tool companies protested that the recommendation on limiting some technologies to allies might cut them out of many markets.

The subcommittee and the House International Relations Committee are considering renewal or replacement of the Export Administration Act which controls foreign trade. It expires Sept. 30.

Testifying before the House committee on March 11, a Harvard expert, Graham Allison, said "the current system is not achieving the U.S. national security objective for which it is designed. It fails to prevent shipment to the Soviet Union of technological products of potential concern to the United States, while restricting U.S. companies from selling many products of no strategic importance."

The system, created more than two decades ago and modified several times since then, links North Atlantic Treaty Organization nations, except Iceland and Japan, in a coordinating committee known as CoCom to control trade with Communist nations.

"The U.S. exporter to Communist countries is still confronted with greater barriers than his counterparts in other Western countries," a Library of Congress specialist, John P. Hardt, told the House committee. J. Fred Bucy, chairman of the Pentagon task force, noted in a memo with the report that "it is always going to be difficult to obtain full cooperation on technology issues from CoCom member nations."

Pressures from West European businessmen eager to make money in the East sometimes override security considerations as viewed from the Pentagon, a senior official there said recently. So does U.S. domestic political pressure, as in the American decision at the warmest period

of detente to help build the world's largest heavy truck plant on the Kama River east of Moscow despite Pentagon objections.

Between 1969 and 1971, the Soviet Union decided to increase greatly its importation of Western technology to try to overcome industrial problems and speed up modernization. "Transfer of advanced technology from Western industrial nations has been perceived by current Soviet leaders as a significant factor in reaching priority targets," one expert study says.

According to an academic estimate, Western technology and equipment imported between 1968 and 1973 enabled the Soviet Union to increase industrial production by some 15 per cent.

The legislation on U.S. trade was loosened in 1972 to remove controls except when their absence "would prove detrimental to the national security of the United States." When renewed in 1974, the law increased Pentagon powers to review exports that would "significantly increase the military capability" of a Communist country.

Bucy's task force was appointed to study the way this worked. As executive vice president of Texas Instruments Inc., a leading electronics firm, Bucy had a reputation of taking a fairly hard line on Communist trade. The task force's report therefore surprised some observers with its drastic new approach which amounted to liberalization in some aspects.

Selling machines and products to the Communists is not the main danger of helping them grow stronger to the possible detriment of the West, the report said. "Design and manufacturing know-how are the principal elements of strategic technology control," it said.

Therefore, primary emphasis in control efforts should be placed on "arrays of design and manufacturing information that include detailed 'how to' instructions . . . plus significant teaching assistance. . . . 'keystone' equipment that completes a process line and allows it to be fully utilized . . . (and) products with technological know-how . . . accompanied by sophisticated information on operation, application, or maintenance."

The report was especially opposed to "turnkey" projects in which a foreign company builds a factory, gets it running while training local people, and then turns it over. The Soviet Union and China have ordered a number of these in the last decade from U.S., British, West German and other firms.

"To preserve strategic U.S. lead time," the report said, "export should be denied if a technology represents a revolutionary advance to the receiving nation, but could be approved if it represents only an evolutionary advance."

"The U.S. should release to nonallied, non-Communist countries only the technology we would be willing to transfer to Communist countries directly," said the recommendation that agitated some manufacturers. "This rule should extend to such technology embodied in weapon sales."

It adds that "any CoCom nation that allows such technology to be passed on to any Communist country should be prohibited from receiving further strategic know-how."

[From the Washington Star, July 13, 1976]

Security of Our Schools: Big Business Gets Bigger

(By Abbott Combes)

School Trek has voyaged to Alexandria.

But only in a manner of metaphor-mixing—it's really the annual convention of the National Association of School Security Directors (NASSD) and science reality, not fiction, is the destination of the Trek. Computers, not phasers.

Space Age electronics has a habit of turning fiction into reality, just as America has a habit of turning developing needs into developing industry, and so the school building guard is on his way in from the cold.

School crime may have declined by $1 million locally this last year (down to $2.25 million) but nationally it's still growing by bricks and break-ins—losses are expected to surpass $600 millon (compared to $594 million the year before).

School security is big business growing bigger.

Thus, as the conventioneers shuttled between conferences on the headier stuff of schoolyard crime, the dollars-and-cents exhibitors, without whom a convention isn't a convention, were pushing their buttons, or trying to.

Bleeps bleeped, microwaves microwaved, multiplexes multiplexed, transceivers transceived, printers printed, flashes flashed—it was School Trek.

Surprisingly, at least to an observer with less than a passing knowledge of such circuital wizardry, most people seemed to know what the salesmen were talking about.

Among the products from the Schoolship Security (in no particular order): Sonitrol, Modular Command, Teletale, Cable Fault Locator, Modular Multiplexer, Motion Detection System (ultrasonic and otherwise), Microwave Intruder Detectors (of various sizes, shapes, ranges and, presumably, colors), Silent Communications Alarm Network, Decoding Alarm Receivers, Fixed Alarm Transmitters and Alarm Relay Unit, Signal Repeaters, Dual Unit Charger, Key Control Protector, Printer Clock Alarm Monitor System, Multipoint Alarm System, Safety Strobe Beacon, Moderne II, to name but a few.

Moderne II, it should be pointed out, is a door hinge. And the Silent Communications Alarm Network is a transmitter in the guise of a fountain pen that the teacher triggers as she is being assaulted.

Explanation of the other hardware is best left to the professionals.

Not everyone was totally enthralled by the electronics. "I get tired of hearing about hardware," complained Stan Rideout of the Pittsburgh school system as he moderated a seminar on "Successful Programs for Controlling School Crime."

An advocate of "Student Power," he urged greater use of the kids themselves in preventing school crime. He cited Pittsburgh's Student Vandalism Patrol, whose motto is, "Instead of throwing a stone, throw a ball. Instead of picking up a stick, pick up a bat."

When a show of hands indicated that the student role in most school districts was limited to participation in committing the crime—not in its prevention—he observed, "It's very sad today that in most of America we're still using the repressive type of cop. . . ."

Other lights, high and low, from a day at the convention (held at the Ramada Inn and continuing through Friday):

Leroy Hostetter, security supervisor for Montgomery County, believes such security personnel are "an embarrassment" to school systems because administrators prefer not to acknowledge vandalism and violence within their domains.

According to "Hostetter's Law," vandals are extremely risk-wise. With no alarm system, they will strike when the school is closed—less risky. When the installation of an alarm system gets results in nabbing kids, they are more willing to accept the risk of open-air delinquency during school hours.

At Walt Whitman High School, 110 public address speakers, "which you can't very well hide in a vest pocket," disappeared during school hours in 1975. Alarm systems treat symptoms, he said, but the cure is education.

The convention has drawn some 250 security specialists, a medley of ex-cops-turned-school-security-aces and educators, from 30 states and Canada. Fifteen of them are women.

All told, the association has about 350 regular members, each representing a school district, and 40 associate (manufacturers, suppliers, etc) members. Officials say NASSD is adding 100 new members a year.

[From the Washington Post, Sept. 23, 1976]

Electronic Wizards Who Have Something To Crow About

Our uncle was an electrical engineer, and he published a book on some complicated something-or-other around the time we arrived on earth. In the inscription, Unc wrote that he was sure our parents would never understand the contents, but perhaps we would some day.

It's a good thing Unc never backed his hunch. Our hopelessness at things electronic is firmly established. But it has not trampled our fascination with machines that go bleep in the night. So we eagerly volunteered to attend last week's convention of the Association of Old Crows at the Sheraton Park Hotel.

That is not a non sequitur. The AOC is a social club, six parts civilian and four parts military, and 10-out-of-10 in the business of electronic warfare. The Crows are the birds who, beginning during World War Two, have developed all the electronic gear, offensive as well as defensive, used by this country, in wartime and out.

The words "electronic warfare" are to an extent misleading. The Old Crows do not build weapons. Nor does all their work have to do with war. They prefer to speak of tools and aids—guidance systems that get fighter jets home again, jamming systems, systems that resist jamming, systems that listen, systems that absorb and analyze.

The Crows' name derives from the British World War Two operatives whom Churchill called his "wizards." They were the men who

deduced that German bomber pilots were locating London by the intersection of two radio beacons. The "wizards" skewed those beams so bombs landed in pastureland. The code name for the British men and mission was "raven," and that has since been whimsicalized into Crows.

Warren Austin of Alexandria is the president Crow. We met him for a cocktail in the cavernous basement of the hotel. All around were displays of the sights and sounds of electronic warfare (EW). One could understand all the interest when Austin began by telling us that the Defense Department is spending $1 billion this fiscal year on EW development, the highest total ever.

"Vietnam is where we proved that EW worked," Austin said. "You can't see it, smell it or feel it, but it did the job.

"I'll give you an example. We developed pods for airplanes. They attach to the wing, and they jam enemy radar tracking signals. The pilots used to complain about carrying the extra weight. They wanted more fuel. But we knew we had it made when two pilots fought one day over whose turn it was to carry the pod."

There are three basic kinds of EW, Austin explained: electronic countermeasures (used to jam or upset enemy EW), electronic support measures (intelligence-gatherers) and electronic counter-countermeasures (used to jam enemy jams, for example).

The absence of a shooting war has not slowed research in any of the three areas, Austin told us, and he insisted that it should not. "One of our constant worries is getting enough money (from Congress) to get on with what needs to be done," he said.

We heard much the same argument when we chatted with marketing executives of three major government contractors—RCA, Sperry-Univac and Adams-Russell.

Edgar Waldron of RCA pointed out that much of the cost of developing new methods of electronic warfare is eventually redeemed in civilian life. He cited color television and microwave ovens as examples. C. M. Jones of Adams-Russell said all the Research and Development expense "is really to prevent war." F. W. Hennin of RCA stressed preparedness. "We've got a big electronic war going on right now," Hennin told us. Intelligence about the Russians and Chinese is essential, he said, "because if you don't know what's going on across the street, you're in trouble."

The men said they are usually abreast of, if not always ahead of, what they all unfailingly call "the enemy." None was especially excited by the defection earlier this month of a Russian pilot who flew his top-secret MIG-25 fighter jet to Japan and was later given asylum in the United States. "When we check that plane," Hennin said, "it'll only tell us what we already know. I'll bet only 10 percent of it will be a surprise." Why so? "Intelligence," Hennin replied.

There are 8,500 Old Crows, up considerably from the 400 who started the club in 1963. Most live here, in California and in Dayton, Ohio, all areas where EW is a big source of employment. The Crows are a serious and dedicated lot, as one might expect, but also fun-loving, as one might not. Listed among the officers of the convention was a golf chairman. Signs advertising "dis-crow-theques" were easily found in the lobby. And, yes, the Old Crows drink their namesake bourbon, among other things.

Their socializing was a bit dampened this year, however, by a new Defense Department regulation. "Air Force 30: 30" prohibits military personnel who deal directly with civilian businessmen from socializing directly with them. It is all to avoid the appearance of "sweetheartism" in the dishing out of government dollars. At the Crows' banquet, "30:30" forced six officials to spend two days pre-assigning 2,500 dinner table seats. But it all worked in the end, amid much complaining and much compliance.

The banquet speeches were mostly hilarious.

The master of ceremonies made a lot of self-conscious jokes about EW appropriations, most of which are provided by the three Senators—Robert Byrd, Howard Cannon and John Tower—who happened to be sitting at the head table.

Army Undersecretary Norman R. Augustine, the keynote speaker, was uproariously insulting. Byrd played "Cripple Creek" and "Cumberland Gap" on the fiddle. Rep. William Dickinson (R-Ala.) brought down the house with Wayne Hays and Jimmy Carter jokes.

There were two silences. One came when the colors were marched in. The other came during the invocation, delivered by Tower. "Bless this organization," Tower said, "dedicated to preserve Thy divine peace through strength."

ROBERT F. LEVEY.

[From the Washington Star, Oct. 29, 1976]

U.S. APPROVES STRATEGIC COMPUTER SALE TO CHINA

President Ford, approving less than standard safeguards and making an exception to prevailing policy, has approved the sale to China of a computer system with military as well as industrial capability.

High administration officials said the sale of two Control Data Corp. Cyber 172 computers and associated equipment was approved as a gesture of support to the new Chinese leadership.

The officials said the United States did not intend to sell the computer system to the Soviet Union, and the deal was an exception to the policy of selling to one of the Communist superpowers only what would also be sold to the other.

A National Security Council memorandum dated Oct. 12 and obtained by Aviation Week and Space Technology had recommended the lesser safeguards and the policy exception on the ground of overriding foreign-policy interests.

A State Department spokesman confirmed the decision to grant an export license. Negotiations to complete the deal are still under way between Control Data and the Chinese government.

American approval, pending for more than a year, was finally given over the objections of the Energy Research and Development Administration. The agency, which is responsible for the nuclear weapons program, said the computer system was used in the United States for making calculations on nuclear tests and could be used by China for the same purpose.

The Pentagon, which had opposed the sale on the ground that the computer system could be used to support radar systems, withdrew its

objections after the State Department agreed to press China to accept safeguards.

These include full access by Control Data personnel to computer centers and full information on computer use and programming. One computer is to be used in China for oil exploration, and the second, to be delivered later, is for seismic exploration. Only one Control Data official would be permitted at the first site for three years and only one at the second site for a limited period of time.

Safeguard standards for sales to Communist countries, including the Soviet Union, provide for blanket monitoring and inspection rights on a continuing basis. The National Security Council memorandum, signed by Lt. Gen. Brent Scowcroft, assistant to the President, acknowledged that the standards in the sale to China were less stringent.

Ford's decision to proceed with the sale runs right up to the line of the permissible limit that he himself drew during the foreign policy debate with Jimmy Carter, the Democratic candidate. Asked whether he would sell military equipment to China, Ford responded:

"I do not believe that we, the United States, should sell, give or otherwise transfer military hardware to the People's Republic of China, or any other Communist nation, such as the Soviet Union and the like."

Advanced computer systems, communications equipment and the like are generally considered to be of the highest potential military value. American officials, in response to queries, are now saying that the Cyber 172 system is not among the more modern ones. When asked about the Cyber 172 and associated equipment a year ago, most officials described it as advanced.

The sales decision is in keeping with Kissinger's assurances to the new leadership in Peking that the United States is interested in China's security relative to the Soviet Union. At a news conference on Friday, he denied that the United States ever had "any defense discussions with China," and said "we believe that the territorial integrity and sovereignty of China is very important to the world equilibrium, and we would consider it a grave matter if this were threatened by an outside power."

Some officials felt that approval of the sale was bound to irritate Soviet leaders. Several Soviet requests to buy computers have been rejected in recent years.

The actual sale of the Cyber 172, if completed, will be made by a French affiliate of Control Data, the Compagnie Generale Geophysique. The estimated cost of the Cyber is said to be $2 million.

[From the New York Times, Oct. 30, 1976]

U.S. Did Not Bar Computer-System Sale to Soviet

(By Leslie H. Gelb)

Washington, Oct. 29.—An executive of Control Data Corporation said today that his company has received Administration approval to sell computer systems of comparable capability to the Soviet Union and China, and this was confirmed by Administration spokesmen.

James J. Bowe, a vice president of Control Data, said that the Cyber 73 computer system being prepared for delivery to the Soviet Union is the equivalent of the two Cyber 172 computer systems approved for sale to China.

The New York Times erroneously reported yesterday that the Administration had no intention of licensing the sale of the same Cyber system to the Soviet Union. Thus, the Administration has not breached its longstanding policy of selling high-technology items to one Communist superpower only if it is prepared to sell comparable items to the other.

Some of the high Administration officials who told The New York Times yesterday that the Cyber system would not be sold to the Soviet Union were contacted today and asked for an explanation.

MILITARY CAPABILITY DENIED

One said that he was completely unaware of the sale to the Soviet Union. Another said that he must have been misunderstood, that he had not meant to imply an exception to policy, but an exception on safeguards.

Mr. Bowe also denied that the Cybers being sold for making calculations on oil exploration and earthquake detection had any value for making calculations for military purposes beyond a hand-held calculator.

He was supported in this view by State Department spokesmen who stated that while any computer could be used for military purposes, the two Cyber models were not of any special or additional value for military programs.

Officials of several different agencies, including the Pentagon and the Energy Research and Development Administration, continued to insist, however, that similar Cyber systems have been used by the United States in making calculations of nuclear tests and in controlling radars.

As one Commerce Department official put it, "If there were no potential military applications there would have been no reason to take a full year to review the sale and no reason to impose safeguards on the use of the equipment."

SAFEGUARDS CALLED ADEQUATE

Officials of every agency involved, with the exception of the Energy Research and Development Administration, said today—as was reported yesterday—that the provisions for monitoring and inspecting the use of the computers were fully adequate to prevent diversion to military uses.

These officials again said that the safeguards in the sale to China were not as stringent as those generally prevailing for comparable transfers of technology.

They said that the principal difference was that whereas the Soviet Union had been required and prepared to give government-to-government assurances that the equipment would have only civilian uses, China was being permitted to give similar assurances to the Control Data Corporation alone. They related that China has been unwilling

to give government-to-government pledges so long as the United States retained diplomatic relations with the Republic of China on Taiwan.

Other deviations from prevailing practices purportedly have to do with some minor details regarding supervision and servicing of the computers.

KISSINGER SAID TO BE INVOLVED

A variety of officials again confirmed that Secretary of State Henry A. Kissinger pressed for approval of the sale to China at this time as a gesture to the new Chinese leadership.

The Cyber 172 is described as on the "low end" of the general purpose computers and more than 70 have been sold since it was introduced several years ago. Officials said that the sale of the Cyber 73 to the Soviet Union was approved on Sept. 30 and the Cyber 172 to China on Oct. 12.

President Ford defended the sale today, saying that it had been approved by the concerned agencies. He added that the decision came in the routine course of business and was handled in the customary fashion.

Officials from every agency involved, including the State Department and the White House, said yesterday and today that the decision was anything but routine—in the time taken to make the decision, the disputes and high-level attention.

INFORMATIONAL PRIVACY: CONSTITUTIONAL CHALLENGES TO THE COLLECTION AND DISSEMINATION OF PERSONAL INFORMATION BY GOVERNMENT AGENCIES

*By Lawrence J. Leigh**

When may a person constitutionally challenge the collection of sensitive personal information by government agencies? Under what circumstances does a person have the right to the removal of personal information from official files or the right to require restricted dissemination of personal information? These questions which lie at the heart of an emerging right to informational privacy grow in importance as Americans become increasingly uneasy about the nature and extent of data collected about them by the government.[1]

The average person is likely to be the subject of dozens of separate files compiled by hospitals, educational institutions, criminal justice agencies and tax and financial departments at the federal, state and local level. Among the sensitive data that may be contained in such records are labels such as addicted, arrested, convicted, truant, mentally retarded, delinquent, homosexual and subversive.[2]

Whatever the purposes of governmental recordkeeping, it is usually not too difficult for those gathering information to advance some justifi-

---

* Member, third year class.

1. *See generally* A. WESTIN & M. BAKER, DATABANKS IN A FREE SOCIETY 465-85 (1972). Public opinion surveys taken in the early seventies revealed that a substantial minority of Americans perceived some invasion of personal privacy. [hereinafter cited as WESTIN I].

2. *See generally* A. MILLER, THE ASSAULT ON PRIVACY (1971); A. NEIER, DOSSIER (1975); ON RECORD (S. Wheeler ed. 1969); A. WESTIN, PRIVACY AND FREEDOM (1967) [hereinafter cited as WESTIN II]. In the mid-sixties, federal files contained over 3 billion records on individual citizens including 264.5 million criminal histories, 279.6 million mental health records, 916.4 million profiles on alcoholism and drug addiction, and over 1.2 billion financial records. *Hearings on Federal Data Banks, Computers, and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess. pt. 1, at 574 (1971). For a more recent survey of the nature and scope of 858 federal data banks *see* STAFF OF SUBCOMM. ON CONSTITUTIONAL RIGHTS OF THE SENATE COMM. OF THE JUDICIARY, 93d CONG., 2d SESS. 1 FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS XXXIII-LVIII (Comm. Print 1974).

cation for their activities. Whether the bureaucracy in question is a police department, school, hospital or welfare bureau, the response is likely to be the same—the more known about the people to be dealt with, the greater the likelihood of making an informed decision.[3] But there are several problems with such an answer. Recent studies in information science indicate that too much information can actually inhibit the process of decisionmaking.[4] Information that is irrelevant or only tangentially related to the decisionmaking process may do more harm than good. The potential for misuse is increased by permitting information to fall into the hands of persons either within or without a collecting agency who are not sensitive to the dangers of misinterpretation of the collected data. Scholars and journalists are beginning to supply solid evidence of cases of abuse. The educator whose evaluations are prejudiced as a result of knowing a student's IQ test score[5] or the employer who refuses to hire on the basis of an applicant's raw arrest record[6] are not unfamiliar examples.

The possible adverse consequences to the individual from governmental data collection do not necessarily stop at misuse by others. The impact on an individual's thoughts and actions may by itself be detrimental. Once an individual knows that his activities or thoughts are the subject of a file, his personal creativity and spontaneity may be inhibited.[7] Data gathering activities which involve highly sensitive data may

3. Recent literature classifies records into three basic types: administrative, investigative and statistical. Administrative records contain information relating to a direct transaction between a person and a government agency. Birth records, criminal histories and license records are examples. Investigative records may contain information drawn from administrative records, but usually include additional personal data not relating to governmental transactions. Common examples are personnel files, police intelligence dossiers and probation reports. The primary purpose of investigative files is to assist decisionmaking concerning file subjects. A third type of record, the statistical record, is used to collect information about groups of subjects for planning and management purposes. Census and other public survey files are the most obvious examples. *See* U.S. DEP'T OF HEALTH, EDUCATION, AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 5-6 (1973) [hereinafter cited as HEALTH, EDUCATION AND WELFARE]. At this writing, the uses and abuses of investigative records by federal intelligence agencies are receiving widespread publicity. *See, e.g.*, COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES, REPORT TO THE PRESIDENT 130-50, 240-50 (1975). This note, however, will not be addressed solely to privacy issues surrounding investigative records, but will extend to administrative and statistical records as well.

4. Ackoff, *Management Misinformation Systems*, 14 MANAGEMENT SCI. B-147 (1967); Altman, *Juvenile Information Systems: A Comparative Analysis*, 24 JUVENILE JUSTICE 2 (Feb. 1974); Bartlett & Green, *Clinical Prediction: Does One Sometimes Know Too Much?*, 13 J. COUNSELING PSYCHOLOGY 267 (1966).

5. *See, e.g.*, Mercer, *IQ: The Lethal Label*, 6 PSYCHOLOGY TODAY 44 (Sept. 1972).

6. *See, e.g.*, H. MILLER, THE CLOSED DOOR: THE EFFECT OF A CRIMINAL RECORD EMPLOYMENT WITH STATE AND LOCAL PUBLIC AGENCIES (1969).

7. Askin, *Surveillance: The Social Science Perspective*, 4 COLUM. HUMAN

engender thoughts or feelings which the subject not only wishes to withhold from others, but that he also is trying to keep from his own consciousness. Personality testing is a specific example of this type of information collection.[8] The anxiety created by knowledge that the state possesses information which, if disclosed, will expose a person to public shame or ridicule cannot be lightly dismissed.[9]

Recent federal[10] and state[11] legislation has granted individuals access to a wide variety of records concerning them, including educational, medical, financial and employment files. As individuals become aware of their right to review the contents of such files, litigation concerning the retention or dissemination of personal data will undoubtedly increase. The purpose of this note is to present a constitutional theory of informational privacy to assist those lawyers and judges who will be faced with such litigation.

I. A Right to Informational Privacy

A. The Supreme Court and the Right to Privacy

Federal Circuit Judge Shirley M. Hufstedler has accurately noted that "[n]o corner of the privacy field is more unkempt than that tended by the United States Supreme Court."[12] Certainly the concept of privacy has been applied in the protection of a variety of interests. But the protection has also been uneven. Consider, for example, the Fourth Amendment which states in part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated . . . ."[13] There is little doubt that the amendment provides considerable protection against indiscriminate rummaging by police through the dwelling places and personal effects of private persons.[14] Indeed, by holding that a violation of the amendment may occur whenever there is an invasion of a

---

Rights L. Rev. 59 (1972); Benn, *Privacy, Freedom, and Respect for Persons*, in Privacy 1 (J. Pennock & J. Chapman eds. 1971).

8. Sherrer & Roston, *Some Legal and Psychological Concerns about Personality Testing in the Public Schools*, 30 Fed. B.J. 111 (1971).

9. Westin II, *supra* note 2, at 33-34.

10. Freedom of Information Act, 5 U.S.C. § 552 (1970); Privacy Act of 1974, 5 U.S.C.A. § 552a (Supp. I, 1976); 20 U.S.C.A. § 1232g (Supp. I, 1976); 42 U.S.C.A. § 3771 (1973).

11. *See, e.g.*, Iowa Code Ann. § 749B.5 (Supp. 1975); Minn. Stat. Ann. § 15.165 (Supp. 1975); Law Enforcement Assistance Administration, Compendium of State Laws Governing the Privacy and Security of Criminal Justice Information (1975).

12. S. Hufstedler, The Directions and Misdirections of a Constitutional Right of Privacy 11 (1971) [hereinafter cited as Hufstedler].

13. U.S. Const. amend. IV.

14. *See, e.g.*, Stanford v. Texas, 379 U.S. 476 (1965).

justifiable or reasonable expectation of privacy[15] the Supreme Court has extended protection far beyond traditional cases of illegal trespass by police.[16]

But the words "searches and seizures" in the Fourth Amendment are, nonetheless, terms of limitation.[17] Governmental information gathering practices which do not involve either a search or seizure are not proscribed by the amendment.[18] This leaves governmental officials considerable freedom to collect information. For example, neither the mere receipt of information from a person who is not an agent of the state,[19] nor the observation of the physical characteristics of an individual in a public place[20] are considered searches or seizures under the amendment. As a general rule, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[21] Consequently, an Internal Revenue summons to an accountant to produce his client's business records does not infringe upon the guarantee of the client's reasonable expectation of privacy.[22] The Fourth Amendment, moreover, is governed by a rule of reasonableness; it proscribes only *unreasonable* searches and seizures.[23] It is not unreasonable, for example, for a congressional statute to require that all foreign currency transactions over $5,000 be reported to the Treasury Department.[24] Finally, Fourth Amendment rights are personal rights which may not be vicariously asserted. A party whose rights are not violated apparently has no standing to contest an illegal search or seizure no matter how detrimental the information collected is to him.[25]

---

15. United States v. White, 401 U.S. 745, 751-52 (1971); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

16. *See* Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 356-409 (1974).

17. *Id.* at 356.

18. *See* United States v. Dionisio, 410 U.S. 1 (1973). In *Dionisio* the Court held that neither a subpoena to appear before a grand jury nor an order to produce a voice exemplar were seizures under the Fourth Amendment. Therefore, they did not have to meet the amendment's test of reasonableness. *Id.* at 8-15. *But see* Nixon v. Sampson, 389 F. Supp. 107 (D.D.C. 1975), *entry of order stayed sub nom.* Nixon v. Richey, 513 F.2d 427 (D.C. Cir. 1975); see note 109 *infra.*

19. Coolidge v. New Hampshire, 403 U.S. 443, 487-90 (1971).

20. *See* Draper v. United States, 358 U.S. 307, 309-10, 313 (1959).

21. Katz v. United States, 389 U.S. 347, 351 (1967).

22. Couch v. United States, 409 U.S. 322, 335-36 (1973).

23. In many situations search and seizures will be reasonable only if they are pursuant to a valid search warrant. United States v. United States Dist. Ct., 407 U.S. 297 (1972); Katz v. United States, 389 U.S. 347 (1967).

24. California Bankers Ass'n v. Shultz, 416 U.S. 21, 59-63 (1974).

25. Brown v. United States, 411 U.S. 223, 229 (1973). In *Brown* the Supreme Court held that where the defendants were not on the premises at the time of the police

These illustrations are not intended to present a definitive outline of the Fourth Amendment but only to demonstrate that its restraints are limited. Whatever it may become in the future,[26] at present Fourth Amendment law does not encompass a general constitutional right to privacy.[27] Not only does it provide limited protection against the overly broad collection of personal information, but it provides practically no limitation on what officials may do with information they gather by lawful means.

The focus of the Fifth Amendment is narrower still. The privilege against self-incrimination provided by the Fifth Amendment protects only against disclosure of information which would tend to expose a person to a criminal penalty.[28] Its prohibitions do not extend to disclosure of facts which expose an individual to loss of reputation or standing in the community.[29] In addition, the privilege is purely personal and does not apply to information obtained from third parties.[30] As stated by Justice Holmes: "[a] party is privileged from producing . . . evidence, but not from its production."[31] The Fifth Amendment provides no protection where a person is required by statute to submit information unless the disclosure would create a substantial hazard of self-incrimination *and* the statute singles out a select group inherently suspect of criminal activities.[32]

Like the Fifth Amendment, the First Amendment contains significant restrictions on governmental efforts to obtain information, but there are limits to its protection as well. The Supreme Court has adopted the strict scrutiny test in cases involving the governmental collection and

search nor had any proprietary interest in the premises, they did not have standing to challenge the propriety of the search.

26. Judge Hufstedler has suggested an increased emphasis on the Fourth Amendment's guarantee of security of person so that "any governmental probe, corporeal or incorporeal, designed to uncover or to disclose information about a person would be a 'search.'" HUFSTEDLER, *supra* note 12, at 26. See also text accompanying note 109 *infra*.

27. Katz v. United States, 389 U.S. 347, 350 (1967).

28. Kastigar v. United States, 406 U.S. 441, 444-45 (1972).

29. Brown v. Walker, 161 U.S. 591, 605-06 (1896).

30. Couch v. United States, 409 U.S. 322, 328 (1973).

31. Johnson v. United States, 228 U.S. 457, 458 (1913).

32. California v. Byers, 402 U.S. 424, 427-31 (1971). In *Shapiro v. United States*, 335 U.S. 1, 32-36 (1948), the Supreme Court held that the mandatory preservation of business records for governmental examination to facilitate price regulation did not violate the Fifth Amendment. The Court restricted the scope of *Shapiro* in *Marchetti v. United States*, 390 U.S. 39 (1968), holding that failure to supply certain wagering information in connection with a federal gambling tax was justified under the Fifth Amendment. The Court noted that the information required was not customarily kept, that the records had no public record aspects, and that the requirements were directed at a "'selective group inherently suspect of criminal activities.'" *Id.* at 57. *See also* Grosso v. United States, 390 U.S. 62, 67-68 (1968).

79-064 O - 76 - 76

disclosure of information about the associations of private individuals. Absent a compelling state interest, the government cannot compel an organization to disclose its membership lists[33] or an individual to disclose the organizations[34] to which he belongs. However, these decisions are based on factual situations where the government has required the subject himself to supply the information, and recognize only a right of privacy in one's associations. They do not necessarily bring the collection and disclosure of other types of information obtained from third parties within the ambit of First Amendment protection.[35]

As the foregoing discussion indicates, the Fourth, Fifth and First Amendments guarantee certain individual rights which may not be infringed by the collection and use of information by the government. But the limited scope of these protections raises several unsettling questions. If official practices relating to the gathering and use of personal information do not invade the First, Fourth or Fifth Amendment rights of the subject of the information, may the government collect, store or transmit such information without restriction?

Specifically, may it require an individual to disclose nonassociational, nonincriminating personal information no matter how sensitive?

May it engage in unrestricted collection of personal information from sources other than the subject of the information?

May it maintain and store personal information without taking any special precautions to preserve its confidentiality?

May it engage in the unrestricted dissemination of personal information?

A partial answer to these questions is found in the guarantees of procedural due process of the Fifth and Fourteenth Amendments. In *Wisconsin v. Constantineau*,[36] the Supreme Court held that local officials could not post notices that sales and gifts of liquor to certain persons were forbidden unless these individuals were given adequate notice and hearing. The Court indicated that whenever stigmatizing personal information is publicly disclosed, notice and an opportunity to

33. Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539 (1963); Louisiana *ex rel.* Gremillion v. NAACP, 366 U.S. 293 (1961); Bates v. City of Little Rock, 361 U.S. 516 (1960); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958).

34. DeGregory v. Attorney General of New Hampshire, 383 U.S. 825 (1966); Shelton v. Tucker, 364 U.S. 479 (1960). Nor may the government absent a legitimate state interest withhold a benefit, such as a license to practice law, for refusal to answer questions about personal associations. Baird v. State Bar of Arizona, 401 U.S. 1 (1971). Although the opinion of the Court in *Baird* did not use the phrase "compelling state interest," it did indicate that the state had a "heavy burden" to show that the inquiry was necessary. *Id.* at 6.

35. See cases cited notes 33, 34 *supra.*

36. 400 U.S. 433 (1971).

be heard may be essential.[37] There will, however, be occasions where personal information should neither be collected nor disseminated irrespective of the adequacy of procedural safeguards. In such situations *Constantineau* is of no assistance to those seeking relief.

A partial answer to these questions is also found in the general constitutional right of privacy first articulated in *Griswold v. Connecticut*.[38] In that case, the Supreme Court struck down a state statute forbidding the private use of contraceptives. In so doing, it held that a constitutional zone of privacy exists in addition to the specific guarantees of the Bill of Rights.[39] Expanding the doctrine in *Roe* v. *Wade*,[40] the Court declared that the decision to have an abortion, at least in the early periods of pregnancy, is within the zone of protected privacy. It stated that fundamental rights of privacy may not be abridged absent a compelling state interest.[41]

Whether the right of privacy is located in the general language of the Ninth Amendment or emanates as a penumbra from the First, Third, Fourth, Fifth and Ninth Amendments, or is inherent in the concept of liberty contained in the Fourteenth Amendment, is a subject of some dispute, as are the precise contours of the right itself.[42] At present, the right includes, but is not necessarily limited to, "the personal intimacies of the home, the family, marriage, motherhood, procreation, and child rearing."[43] In its privacy decisions the Court has confined itself to the discussion of the right of individual autonomy, and has not addressed the right of informational privacy.[44]

---

37. Justice Douglas speaking for the Court stated that "[w]here a person's good name, reputation, honor, or integrity is at stake because of what the government is doing to him, notice and an opportunity to be heard are essential." *Id.* at 439. *Cf.* Doe v. McMillan, 412 U.S. 306, 323-24 (1973). At this writing, the Court has just granted certiorari in another case involving allegedly stigmatizing information. Davis v. Paul, 505 F.2d 1180 (6th Cir. 1974), *cert. granted*, 421 U.S. 909 (1975) (No. 891, 1974 Term). The plaintiff in *Davis* commenced a class action alleging a denial of civil rights as a result of the distribution of a flyer entitled "Active Shoplifter" upon which his name appeared. Relying on *Wisconsin v. Constantineau*, the court of appeals held that "law enforcement officials cannot, consistent with the Due Process Clause, brand a person as an active shoplifter when he has never been tried for the offense." *Id.* at 1184. The outcome of *Davis* could be crucial to the survival of a right to informational privacy. If unfettered dissemination of such damaging and potentially misleading information as raw arrest records is permitted, it will be extremely difficult to sustain any constitutional challenge to the collection and use of personal information.

38. 381 U.S. 479 (1965).

39. *Id.* at 484-85.

40. 410 U.S. 113, 153 (1973).

41. *Id.* at 152-53.

42. *Id.* at 155-56. *See also* Griswold v. Connecticut, 381 U.S. 479 (1965).

43. Paris Adult Theatre I v. Slaton, 413 U.S. 49, 65 (1973) (state law prohibiting the viewing of obscene movies in public theatres does not infringe upon the right of privacy).

44. *Id.;* Roe v. Wade, 410 U.S. 113 (1973); Doe v. Bolton, 410 U.S. 179 (1973);

Individual autonomy refers to the right to determine for oneself whether one will go through or abstain from certain experiences, such as contraception or abortion.[45] On the other hand, informational privacy is, as so well defined by Professor Alan F. Westin, "[the] claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."[46] Informational privacy and individual autonomy, nevertheless, share similar characteristics. Neither is explicitly found in the language of the Constitution, but both appear to be implicit in the specific guarantees found in the Bill of Rights and the Fourteenth Amendment. Both would seem to be part of the classic right to be let alone so eloquently described by Mr. Justice Brandeis in his dissent in *Olmstead* v. *United States*:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.[47]

B. A Case-by-Case Approach

The initial definition of new constitutional concepts is often articulated in forums other than the Supreme Court. Valuable discussion of informational privacy is to be found in the decisions of lower federal and state courts. Such decisions have involved challenges to the collection of criminal justice, medical, educational, welfare and financial information.

1. *Criminal Justice Information*

York v. Story,[48] which predated *Griswold*, is an important circuit court decision on informational privacy. The factual context of this case presented constitutional violations arising not only from the dissemination of information to third parties, but also from mere collection of the information. *York* involved a female complainant who went to

---

Eisenstadt v. Baird, 405 U.S. 438 (1972); Stanley v. Georgia, 394 U.S. 557 (1969). *See also* Note, *On Privacy: Constitutional Protection for Personal Liberty*, 48 N.Y.U.L. REV. 670 (1973) [hereinafter cited as *On Privacy*].

45. *See generally* Beardsley, *Privacy: Autonomy and Selective Disclosure* in PRIVACY 56 (J. Pennock & J. Chapman eds. 1971); *On Privacy*, *supra* note 44.

46. WESTIN II, *supra* note 2, at 7.

47. 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) *cf.* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

48. 324 F.2d 450 (9th Cir. 1963), *cert. denied*, 376 U.S. 939 (1964).

police to report that she had been assaulted. A male officer insisted that she pose for nude photographs although her bruises would not appear in the photographs, and the photographs would not actually be needed in the prosecution of the case. The officer subsequently distributed the photographs to other officers in the department even though the photographs could not have aided in apprehending the offender.

The Ninth Circuit held that the appellant's allegations, if supported by the evidence, demonstrated a violation of her constitutional right to privacy inherent in the due process clause of the Fourteenth Amendment.[49] According to the court, at least three separate aspects of the police conduct were constitutionally objectionable: 1) the actual exposure of the complainant's nude body to the male police officer; 2) the taking and retention of the photographs; and 3) the dissemination of the photographs to the other officers.[50] At the very least, *York* stands for the proposition that government officials acting under color of law may not collect and disseminate personal information for private as opposed to governmental purposes.

A subsequent Ninth Circuit decision restricted *York* to its facts. In *Baker v. Howard*,[51] police questioned an individual about a suspicious incident but concluded that no crime had been committed. They nevertheless released a police report suggesting that the suspect had committed a crime. A radio station published the report and as a result the suspect lost his teaching position. Distinguishing *York*, the court held that "the invasion of privacy here complained of is not . . . so flagrant that it calls for invocation of the Constitution."[52] Not all courts

49. *Id.* at 456.

50. *Id.* at 455-56.

51. 419 F.2d 376 (9th Cir. 1969).

52. *Id.* at 377. Courts appear to be much more reluctant to find a right of privacy where an individual has been suspected of involvement in crime or has been convicted. In Rosenberg v. Martin, 478 F.2d 520 (2d Cir.), *cert. denied*, 414 U.S. 872 (1973) the court reversed the trial court and dismissed a complaint filed by a person convicted of murder who alleged that police officials disseminated libelous and slanderous information about him before and after he was taken into custody. In Travers v. Paton, 261 F. Supp. 110 (D. Conn. 1966), the district court held that the shooting and subsequent televising of a film of a parol hearing of a state prison inmate did not violate the inmate's constitutional right of privacy. The court distinguished *York* on the grounds that the intrusion was not "shocking." *Id.* at 115. *See also* Mimms v. Philadelphia Newspapers, Inc., 352 F. Supp. 862 (E.D. Pa. 1972); Mattheis v. Hoyt, 136 F. Supp. 119 (W.D. Mich. 1955). However, the constitutional right of privacy has been cited to deny defense counsel the right to administer an anonymous questionnaire to grand jurors for purposes of showing underrepresentation by age and social class. People v. Super. Ct. (Dean), 38 Cal. App. 3d 966, 976, 113 Cal. Rptr. 732, 739-40 (1974); *see also* People v. Norman, 76 Misc. 2d 644, 651, 350 N.Y.S.2d 52, 60 (Sup. Ct. 1973) (discovery of police officers' personnel records for impeachment purposes absent a showing of more than mere speculation by the defense is tantamount to an unconstitutional invasion of privacy); *cf.* United States v. Liebert, 519 F.2d 542 (3rd Cir. 1975).

have taken such a benign view of the information-gathering practices of criminal justice agencies. Indeed, some courts have gone beyond *York* to hold that the mere collection and retention of certain information even without dissemination to private parties may be constitutionally impermissible.[53]

In *Davidson v. Dill*[54] the plaintiff was arrested and tried for loitering but was subsequently acquitted. She then brought an action demanding the return of her arrest record. Reversing a lower court dismissal of her complaint, the Supreme Court of Colorado concluded that a court should expunge an arrest record or order its return when the harm to the individual's right of privacy or dangers of unwarranted adverse consequences outweigh the public interest in retaining the records in police files.[55] The court noted that privacy is a fundamental right, and indicated that police officials must demonstrate a compelling state interest in maintaining arrest records.[56] Remanding the case for adjudication on its merits, the court urged the lower court to consider: "[w]ho has access to these records, what facts are contained in them, how likely and to what extent information in the records may be disseminated, and what justification exists for their retention in the police files. . . ."[57]

In a recent California case, *White v. Davis*,[58] the constitutionality

53. *See, e.g.*, cases cited notes 54, 55, 58 *infra*.

54. 180 Colo. 123, 503 P.2d 157 (1972).

55. *Id.* at 130, 503 P.2d at 161. *Accord*, Eddy v. Moore, 5 Wash. App. 334, 487 P.2d 211 (1971); United States v. Hudson, 103 Wash. Law Rep. 377 (D.C. Super. Ct. 1975). *See also* Doe v. Commander, Wheaton Police Dept., 273 Md. 262, 329 A.2d 35 (1974). *But see* Monroe v. Tielsch, 84 Wash. 2d 217, 525 P.2d 250 (1974). *Contra*, United States v. Linn, 513 F.2d 925 (10th Cir.), *cert. denied*, 18 Cr. Law Rep. 4013 (U.S. Oct. 8, 1975); Herschel v. Dyra, 365 F.2d 17 (7th Cir.), *cert. denied*, 385 U.S. 973 (1966); United States v. Seasholtz, 376 F. Supp. 1288 (N.D. Okla. 1974); United States v. Dooley, 364 F. Supp. 75 (E.D. Pa. 1973); Coalition of Black Leadership v. Doorley, 349 F. Supp. 127, 130 (D.R.I. 1972); Beasley v. Glenn, 110 Ariz. 438, 520 P.2d 310 (1974).

In *Tosh v. Buddies Supermarkets, Inc.*, 482 F.2d 329 (5th Cir. 1973), local police officials furnished the criminal histories of union organizers to the management of a supermarket which had been the scene of incidents in which the organizers were involved. The court held that the Constitution did not ban a state agency from furnishing such information to the supermarket management since it had a legitimate need for the information. *Id.* at 332.

The general issue of expungement of arrest records and the various approaches toward resolution of the problem is a vast subject beyond the scope of this note. *See generally* Note, *Criminal Procedure: Expunging the Arrest Record When There Is No Conviction*, 28 OKLA. L. REV. 377 (1975); Comment, *Retention and Dissemination of Arrest Records: Judicial Response*, 38 U. CHI. L. REV. 850 (1971).

56. Davidson v. Dill, 180 Colo. 123, 130, 503 P.2d 157, 161 (1972).

57. *Id.* at 132-33, 503 P.2d at 162.

58. 13 Cal. 3d 757, 533 P.2d 222, 120 Cal. Rptr. 94 (1975).

of police intelligence activity at the University of California at Los Angeles was challenged. Plaintiffs sought a permanent injunction against the Los Angeles Police Department to prevent undercover officers from attending discussions in university classes and in public and private meetings of university-sponsored organizations for the purpose of compiling intelligence reports. A lower court sustained a demurrer to the plaintiffs' complaint and entered judgment for the defendants. Noting that the complaint alleged that the information gathered by the police did not pertain to illegal activity, the California Supreme Court ruled that the lower court erred in sustaining the demurrer.[59] The court held that absent a compelling state interest which was not revealed in the pleadings, the stationing of undercover agents in classrooms and the extensive collection of information about members of the university community violated the First Amendment[60] and a state constitutional right to privacy.[61] It also implied that the police practices violated the federal right to privacy as well.[62] *White* illustrates the potential overlap in protection which the First Amendment and the right of privacy provide when the information collected relates to beliefs or associations.[63] As both *York v. Story*[64] and *Davidson v. Dill*[65] demonstrate, that overlap is not present in every case, since much information collected and retained by criminal justice agencies has nothing directly to do with the exercise of First Amendment rights.

2. *Health and Medical Information*

In *Roe v. Ingraham*,[66] patients and physicians challenged a New York statute which required physicians to file copies of prescriptions for certain drugs with the state department of health. A federal district court dismissed the complaint, which alleged that the statute violated the plaintiff's constitutional right to privacy,[67] for lack of a substantial

59. *Id.* at 760, 533 P.2d at 224, 120 Cal. Rptr. at 96.

60. *Id.* at 772-73, 533 P.2d at 232, 120 Cal. Rptr. at 104.

61. *Id.* at 776, 533 P.2d at 234-35, 120 Cal. Rptr. at 106-07. *See also* CAL. CONST. art. I, § 1.

62. White v. Davis, 13 Cal. 3d 757, 775, 533 P.2d 222, 234, 120 Cal. Rptr. 94, 106 (1975).

63. *See also* Comment, *Police Surveillance of Political Dissidents*, 4 COL. HUMAN RIGHTS L. REV. 101 (1972).

64. See text accompanying notes 48-50 *supra*.

65. See text accompanying notes 54-57 *supra*.

66. 480 F.2d 102 (2d Cir. 1973).

67. *Id.* at 105. In *Felber v. Foote*, 321 F. Supp. 85 (D. Conn. 1970), a case arising prior to *Roe v. Wade*, the district court held that a psychiatrist had no right to declaratory and injunctive relief from enforcement of a state statute requiring him to report the names and other personal information of drug dependent patients to the state department of health. The court concluded that there was no general constitutional right of privacy. *Id.* at 89. The California Supreme Court in *In Re Lifschutz*, 2 Cal. 3d 415,

federal question. The Second Circuit reversed and remanded, holding that the disclosure of the information mandated by the statute presented a substantial constitutional question of invasion of privacy.[68] The court stated:

> If there is anything "obvious" about the constitutional right to privacy at the present time, it is that its limits remain to be worked out in future cases. Should the constitutionally protected zone of privacy be extended beyond the area already recognized, the individual's interest in keeping to himself the existence of his physical ailments and his doctor's prescriptions for them would lie rather close in the continuum. If New York had passed a statute directing that all prescriptions, or even all prescriptions for Schedule II drugs, must be published in the press, we do not think the State would have seriously contended, still less that the district judge would have held, that a constitutional attack was "obviously frivolous."[69]

New York had argued that the central filing of the prescriptions was necessary to detect negligent or intentional over-prescription of dangerous drugs by doctors. While acknowledging that the state had advanced a powerful argument for sustaining the statute, the court nonetheless urged consideration by a three-judge court of how the confidentiality of the information was actually being preserved.

> If it were clear that the State had taken or proposed to take effective steps, by regulation or otherwise, to limit access to the patients' names on the prescription forms as rigidly as is consistent with accomplishment of the asserted statutory purpose, the grounds for constitutional attack might disappear. But the district court was not entitled to dismiss the complaint on the basis of the State's assertions that it has already done this.[70]

The above language strongly suggests that a sharing of the information with other governmental agencies for purposes not related to its collection may be prohibited.

On remand, however, the relevancy of the information rather than safeguards insuring its confidentiality became the critical issue. A

424, 467 P.2d 557, 562, 85 Cal. Rptr. 829, 834 (1970), held that a psychiatrist could not constitutionally refuse to disclose his patient's treatment records in a personal injury suit where the patient failed to challenge such disclosure. The court observed that the psychiatrist's privacy interest apart from that of his patient was not significant. In *Association of American Phys. & Sur. v. Weinberger*, 395 F. Supp. 125 (N.D. Ill. 1975), the district court held that a statute which required physicians to report information on patients to nonprofit professional associations charged with the responsibility of overseeing funds paid under medicare or medicaid did not violate the physician's right of privacy. A critical factor in the court's decision was the statutory provision that the confidentiality of the information be maintained, and that persons seeking unauthorized access to the information be subject to criminal sanctions. *Id.* at 135-37.

68. Roe v. Ingraham, 480 F.2d 102, 109 (2d Cir. 1973).

69. *Id.* at 108.

70. *Id.* at 109.

three-judge federal district court declared that the doctor-patient relationship was within the constitutional zone of privacy, and held that the state's regulatory scheme was unnecessarily broad.[71] The court concluded that the state could determine whether there was over-prescription of dangerous drugs from reports by physicians without knowing the name of the person receiving the drugs.[72] Experience under the prescription reporting program revealed that official knowledge of the patient's name contributed nothing to the objectives of the statute.

Schulman v. New York City Health and Hospital Corp.[73] presents another case involving medical records. In *Schulman*, a gynecologist and a patient who had obtained an abortion at a city hospital center sought to invalidate a city requirement that a pregnancy termination certificate be filed with a central filing registry maintained by the New York City Board of Health. Local health department regulations adopted pursuant to the New York City charter provided that the abortion records would not be subject to subpoena or to inspection by persons other than authorized personnel in the department.

The court noted that the plaintiff possessed a legitimate right of privacy under *Roe*, but held that the assurance of the confidentiality of such information coupled with the state's compelling interest in gathering the information required a rejection of the plaintiff's claim.[74] The principal compelling state interests were 1) to allow followup where medical complications ensue, 2) to enable public health authorities to investigate if proper procedures were followed in an outpatient facility, 3) to provide statistical information as to the effect of multiple abortions on the same woman, 4) to offer public health counseling on family planning and 5) to insure that women who test positive for an Rh negative factor, venereal disease or other factors receive proper counseling and treatment.[75]

In sum, there appears to be little doubt that where the state interest is strong, the collection and retention by appropriate agencies of highly

71. Roe v. Ingraham, 403 F. Supp. 931 (S.D.N.Y. 1975).

72. *Id.* at 938.

73. 44 App. Div. 2d 482, 355 N.Y.S.2d 781 (1974).

74. *Id.* at 486, 355 N.Y.S.2d at 785; *accord,* Planned Parenthood of Central Mo. v. Danforth, 392 F. Supp. 1362, 1374 (E.D. Mo. 1975). In State v. Jacobus, 75 Misc. 2d 840, 348 N.Y.S.2d 907 (Sup. Ct. 1973), the state sought an order enjoining defendant doctors from omitting from certificates of fetal death the name and addresses of parents of aborted fetuses. Such information was used to compile state vital statistics. The court noted that there were no safeguards to insure the confidentiality of the information, which might be subject to subpoena by local district attorneys. For these reasons, the doctors were justifed in their noncompliance with the reporting requirements until the confidentiality of the information could be assured by legislation or other appropriate means. *Id.* at 846, 348 N.Y.S.2d at 913-14.

75. Schulman v. New York City Health and Hospitals Corp., 44 App. Div. 2d 482. 485, 355 N.Y.S.2d 781, 784-85 (1974).

sensitive health and medical records will be permitted.[76] Courts, nevertheless, appear receptive to constitutional arguments that states must take adequate steps to preserve the confidentiality of such records.[77]

3. *Welfare and Educational Information*

In *Merriken v. Cressman*,[78] a mother and her son, a junior high school student, brought an action to restrain the implementation of a school-sponsored drug prevention program. The essence of the program consisted of the administration of questionnaires containing personal questions about parents and family. For example, students were asked whether their parents gave them affection and whether they felt loved by their parents. They were also asked to identify other students who acted unusually, made odd remarks or quarrelled with other students.[79] The findings from the questionnaires were to be utilized at some later time as guide for intervention by school personnel, many of whom were not trained in psychotherapy or psychology. Such intervention was to consist of a form of peer group therapy. The program did not provide specific guidelines for the preservation of the confidentiality of the information which would have been disseminated to various personnel including school superintendents, principals, coaches, PTA officers and school board members.[80] Holding that the program violated the plaintiff's right to privacy inherent in the penumbra of the Bill of Rights,[81] the federal district court noted: "These questions go directly to an individual's family relationship and his rearing. There is probably no more private a relationship, excepting marriage, which the Constitution safeguards than that between parent and child."[82]

In contrast to *Merriken* are decisions involving the constitutionality of statutes which require unwed mothers who receive federal or state assistance to disclose the name of the putative father.[83] The purpose of such disclosure is to enable the state to enforce the father's duty to contribute to the welfare of the child. In such cases plaintiff mothers have objected to disclosure primarily on the ground that it leads to added strain within the home and sometimes results in the permanent separation of the putative father from the rest of the family.[84] Courts in

76. See cases cited note 74 *supra*.

77. *Id.*

78. 364 F. Supp. 913 (E.D. Pa. 1973).

79. *Id.* at 916.

80. *Id.*

81. *Id.* at 922.

82. *Id.* at 918.

83. Doe v. Norton, 365 F. Supp. 65 (D. Conn. 1973), *vacated on other grounds sub nom.* Roe v. Norton, 422 U.S. 391 (1975); Burdick v. Miech, 385 F. Supp. 927 (E.D. Wis. 1974); Saiz v. Goodwin, 325 F. Supp. 23 (D.N.M. 1971).

84. *See, e.g.*, Doe v. Norton, 365 F. Supp. 65 (D. Conn. 1973), *vacated on other*

these cases have held that no fundamental right of privacy prohibits disclosure.[85] The question of preserving the confidentiality of such information once it passes to welfare officials apparently has not been an issue.

4. *Financial and Other Miscellaneous Information*

City of Carmel-By-The-Sea v. Young[86] involved the public disclosure of personal financial information. Plaintiff, City of Carmel, brought an action attacking the validity of a financial disclosure law enacted for the purpose of exposing and minimizing possible conflicts of interest among governmental officials. The California statute required that every public officer and each candidate for state or local office file as a public record a statement describing the nature and extent of his investments, and a similar statement concerning investments in excess of $10,000 owned by his spouse or minor children. The law did not limit disclosure to those financial dealings or assets which could be expected to give rise to a conflict of interest. It mandated disclosure without regard to the nature or location of the assets, or the powers and duties of the officer.[87] The harmful effects of unnecessarily broad disclosure were noted by the court:

> [T]he newspaper publication of a public officer's assets, or those of the spouse or children, can be expected to bring unwanted solicitation from a variety of salesmen and others, could well encourage harassment lawsuits or demands of like nature, and could expose the public officer and family to various criminal elements in our society. Other public officials whose worth or investments do not require disclosure may find that fact understandably embarrassing. The invasion of privacy rights and the chilling or discouraging effect upon the seeking or holding of public office, great or small, or high or low, appears too clear for dispute.[88]

The court declared that the statute violated the United States Constitution.[89] The overly broad compulsory disclosure intruded into the zone of privacy protected by the Fourth Amendment and that "penumbra of constitutional rights into which the government may not

---

grounds sub nom. Roe v. Norton, 422 U.S. 391 (1975). The substantial infringement on privacy inherent in the present welfare system is the subject of empirical inquiry in Handler & Hollingsworth, *Stigma, Privacy and Other Attitudes of Welfare Recipients*, 22 STAN. L. REV. 1 (1969).

85. Doe v. Norton, 365 F. Supp. 65, 77 (D. Conn. 1973), *vacated on other grounds sub nom.* Roe v. Norton, 422 U.S. 391 (1975); Burdick v. Miech, 385 F. Supp. 927, 930 (E.D. Wis. 1974); Saiz v. Goodwin, 325 F. Supp. 23, 26 (D.N.M. 1971). *Cf.* Wyman v. James, 400 U.S. 309 (1971).

86. 2 Cal. 3d 259, 466 P.2d 225, 85 Cal. Rptr. 1 (1970).

87. *Id.* at 269-70, 466 P.2d at 232-33, 85 Cal. Rptr. at 8-9.

88. *Id.* at 270, 466 P.2d at 233, 85 Cal. Rptr. at 9.

89. *Id* at 272, 466 P.2d at 235, 85 Cal. Rptr. at 11.

intrude absent a showing of compelling need . . . ."[90] A more narrowly drawn statute, however, providing for broad disclosure of assets relevant to the duties of public officers and employees would satisfy the constitutional requirement that the least restrictive means be employed where fundamental liberties are concerned.[91]

Four years after *City of Carmel*, the California Supreme Court upheld a second conflict of interest statute written to meet the objections voiced in the earlier decision.[92] Among other things, the new statute required certain designated officials to disclose only those interests which would have a material effect on decisions by the officials acting within the scope of their public duties.[93]

In other states conflict of interest statutes have been sustained on the grounds that broad public disclosure is necessary to further the state's interest in effective government.[94] Courts sustaining such statutes, however, have refrained from denying the possibility that instances may exist where public dissemination of personal financial data might infringe upon an individual's right of informational privacy. In Illinois, for example, state employees challenged the constitutionality of a governor's order requiring them to file as a public record statements of economic interest which included a complete accounting of assets and liabilities.[95] The Illinois Supreme Court held that the sweeping disclosure requirements did not infringe upon the right of privacy.[96] Unlike the California Supreme Court in the *City of Carmel*, the Illinois court concluded that the required disclosure was necessary to further a compelling state interest.[97] The court, however, did not expressly reject the concept of a right of informational privacy relating to financial data.

In addition to challenges to financial disclosure laws,[98] challenges

90. *Id.* at 268, 466 P.2d at 232, 85 Cal. Rptr. at 8.

91. *Id.* at 272, 466 P.2d at 234, 85 Cal. Rptr. at 10.

92. County of Nevada v. MacMillen, 11 Cal. 3d 662, 522 P.2d 1345, 114 Cal. Rptr. 345 (1974).

93. *Id.* at 668-69, 522 P.2d at 1348-459, 114 Cal. Rptr. at 348-49.

94. Illinois State Employees Ass'n v. Walker, 57 Ill. 2d 512, 315 N.E.2d 9 (1974). Stein v. Howlett, 52 Ill. 2d 570, 289 N.E.2d 409 (1972), *cert. denied*, 412 U.S. 925 (1973); Montgomery County v. Walsh, 274 Md. 502, 336 A.2d 97 (1975); Fritz v. Gorton, 83 Wash. 2d 275, 517 P.2d 911 (1974), *appeal dismissed*, 417 U.S. 902 (1974).

95. Illinois State Employees Ass'n v. Walker, 57 Ill. 2d 512, 315 N.E.2d 9 (1974).

96. *Id.* at 526, 315 N.E.2d at 16-17.

97. *Id.*

98. Reference to the privacy issues associated with the collection of financial information was made in a recent United States Supreme Court Case. California Bankers Ass'n v. Shultz, 416 U.S. 21 (1974) (Powell & Blackmun, JJ., concurring). In *California Bankers* the Court, in a six-to-three decision, ruled that federal statutes and implementing regulations requiring financial institutions to report domestic currency transactions over $10,000, and individuals to report foreign currency transactions over $5,000, did not violate the Fourth Amendment rights of those reporting the information. A con-

to collection and dissemination of various types of administrative data have been made within the last decade. Courts have been unsympathetic to attacks on laws mandating the fingerprinting of stockbrokers,[99] mental patients,[100] realtors[101] and gun dealers and transporters.[102] Similarly, regulations requiring that social security numbers be submitted as a condition of obtaining a license to drive[103] and to practice law[104] have been upheld. As to the question of improper dissemination, at least two courts have held that the sale of motor vehicle registration records to private parties does not violate the right of privacy.[105]

C. Emerging Principles

As the foregoing discussion has illustrated, informational privacy questions cut across a wide variety of governmental agencies, records and data collection practices. Moreover courts are in disagreement as to when the right of informational privacy even exists. The danger of mixing apples with oranges while formulating constitutional standards in this area should not be taken lightly. Some courts have tended to equate the right of individual autonomy protected in *Griswold* and *Roe* with the right of informational privacy,[106] but the interests underlying the two rights are, of course, different.[107] When courts do equate the

curring opinion by Justice Powell, joined by Justice Blackmun, however, cautioned that an extension of the regulations would raise "difficult constitutional questions." *Id.* at 78. In their view, "[a]t some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy." *Id.* at 79. Whether Justice Powell was referring to the type of privacy protected by the First or Fourth Amendment or to the general constitutional right of privacy is not clear. The ambiguity in the opinion, however, leaves the impression that any or all of the above constitutional guarantees might apply depending on the circumstances of the case.

99. Thom v. New York Stock Exchange, 306 F. Supp. 1002 (S.D.N.Y. 1969), *aff'd sub nom.* Miller v. New York Stock Exchange, 425 F.2d 1074 (2d Cir.), *cert. denied*, 398 U.S. 905 (1970).

100. Winters v. Miller, 446 F.2d 65 (2d Cir. 1971).

101. Hamilton v. New Jersey Real Estate Comm'n Dep't of Ins., 117 N.J. Super. 345, 284 A.2d 564 (1971).

102. Burton v. Sills, 99 N.J. Super. 516, 240 A.2d 462 (1967).

103. Conant v. Hill, 326 F. Supp. 25, 26 (E.D. Va. 1971) (citing a previous unpublished decision Conant v. Hill, Civil No. 609-70-R (E.D. Va. Mar. 17, 1971).

104. Cantor v. Supreme Court of Pennsylvania, 353 F. Supp. 1307 (E.D. Pa. 1973).

105. Lamont v. Commissioner of Motor Vehicles, 269 F. Supp. 880 (S.D.N.Y. 1967) (claim that dissemination violated right of privacy found insubstantial where information was neither vital nor intimate but rather in the category of public record); Chapin v. Tynan, 158 Conn. 625, 264 A.2d 566 (1969) (per curiam opinion not discussing reasons for sustaining lower court's dismissal of an action for an injunction restraining the commissioner of motor vehicles from selling licensing information).

106. *See, e.g.*, Merriken v. Cressman, 364 F. Supp. 913, 917-18 (E.D. Pa. 1973); Davidson v. Dill, 180 Colo. 123, 131, 503 P.2d 157, 161 (1972).

107. See text accompanying notes 38-46 *supra.*

right of informational privacy with the right of individual autonomy, they commit serious error. Individual autonomy is likely to be restricted to a narrow range of situations dealing with home, family and procreation.[108] Confusion of the two rights may result in decisions similarly restricting the right of informational privacy. This would be unfortunate, since the collection of highly personal information unrelated to home, family and procreation may, nevertheless, involve risk of substantial harm to the individual.

As with the right of individual autonomy, the locus of the right of informational privacy is far from clear. The right would seem to lie somewhere between "liberty" protected by the Fourteenth Amendment and the penumbra of the Bill of Rights. Perhaps its ultimate resting place will be an expansion of the guarantees of the Fourth Amendment.[109] Identifying the precise origins of the right, however, may be

---

108. *See* Paris Adult Theatre I v. Slaton, 413 U.S. 49, 65 (1973).

109. *See* Nixon v. Sampson, 389 F. Supp. 107 (D.D.C. 1975), *entry of order stayed sub nom.* Nixon v. Richey, 513 F.2d 427 (D.C. Cir. 1975); HUFSTEDLER, *supra* note 12, at 26. The unique controversy in *Sampson* involved the ownership of and access to former President Richard M. Nixon's tapes and papers. Mr. Nixon sought an order from the federal district court requiring the federal government to comply with the terms of an agreement concluded shortly after Mr. Nixon left office between Mr. Nixon and Arthur F. Sampson, Administrator of the General Services Administration. The agreement provided for transfer to Mr. Nixon of various tapes and papers of his administration left behind in the course of Mr. Nixon's extraordinary departure from the White House. The special prosecutor, an intervenor-defendant, counterclaimed against Mr. Nixon for declaratory relief asserting the right to access to the president's tapes and papers pursuant to an agreement concluded between the special prosecutor and President Ford on November 9, 1974. Mr. Nixon contended that the November 9th agreement providing the special prosecutor with access violated the Fourth Amendment's prohibition against unreasonable searches and seizures. The court, however, held that the tapes and papers were government property in the government's possession, and therefore, any examination by the special prosecutor pursuant to the November 9th agreement did not violate Mr. Nixon's right to be free from unreasonable searches and seizures. *Id.* at 154-55. The court, nevertheless, held that Mr. Nixon had a right to privacy under the Fourth Amendment with respect to his personal papers and conversations which were intermingled with official tapes and papers. *Id.* at 156-57. In accordance with its holding, the court announced various procedures for the segregation of Mr. Nixon's personal materials from his official papers and tapes and the restriction of government access to the latter. The details of those procedures are of no particular concern to this discussion, but the court's views on the Fourth Amendment are. Its holding is a departure from the theory that there is no Fourth Amendment protection of privacy where there is no unlawful search and seizure. See text accompanying notes 17-27 *supra*. The court's decision implies an independent right of information privacy existing within the guarantees of the Fourth Amendment. In the midst of this litigation, Congress passed the Presidential Recordings and Materials Act, PUB. L. No. 93-526, 88 Stat. 1695 (1974). The act provides for government custody of Mr. Nixon's tapes and papers, and requires the Administrator of the General Services Administration to promulgate regulations to insure the protection of the materials and to specify procedures for access to them. The act also specifies that the regulations shall be formulated with the objective of transferring to Mr. Nixon those presi-

less important than clarifying its meaning, since an abridgement of the right of informational privacy may arise any time personal information is collected, maintained or disseminated.

1. *Improper Collection*

Official collection of information which is unrelated, or only tangentially related to a legitimate governmental function, may violate an individual's privacy rights.[110] Specific examples of improper collection have been shown by *White v. Davis*[111] (involving alleged indiscriminate recording by police of college activities) and *City of Carmel-By-The-Sea v. Young*[112] (involving overly broad collection of financial information for conflict of interest purposes). Moreover, although information may be related to a legitimate governmental function when it is first collected, after a period of time it may be of no use to the collecting agency. In such a case retention of the information would logically violate an individual's right of privacy to the same degree that it would if the information did not have any legitimate use in the first place.[113]

2. *Improper Maintenance and Storage*

Even if information is relevant to governmental functions, its improper maintenance and storage may be constitutionally offensive if the

---

dential materials which neither have historical significance nor pertain to the Watergate incident. When the act became effective Mr. Nixon brought a second suit challenging its implementation. N.Y. Times, Jan. 8, 1976, at 1, col. 1 (city ed.). Subsequently, the court of appeals stayed the district court's order implementing *Nixon v. Sampson* until a three-judge court could decide whether the Presidential Recordings and Materials Act was constitutional. Nixon v. Richey, 513 F.2d 427 (D.C. Cir. 1975). The three-judge court issued its decision just prior to the printing of this note. It unanimously upheld the act, but left open the question of whether Mr. Nixon owned the materials prior to the effective date of the Act. N.Y. Times, Jan. 8, 1976, at 1, col. 1 (city ed.). The court held that although Mr. Nixon had a reasonable expectation of privacy, the act's infringement of such expectation of privacy was reasonable under the circumstances, particularly in view of its provision reserving to Mr. Nixon the sole custody and use of purely personal papers and tapes.

110. *Cf.* Shelton v. Tucker, 364 U.S. 479, 488 (1960).

111. 13 Cal. 3d 757, 533 P.2d 222, 120 Cal. Rptr. 94 (1975).

112. 2 Cal. 3d 259, 466 P.2d 225, 85 Cal. Rptr. 1 (1970).

113. *Cf.* DeGregory v. Attorney General of New Hampshire, 383 U.S. 825, 828-29 (1966) (referring to the "staleness" of information as a consideration for justifying refusal by an individual to provide a legislative committee with information on his earlier involvement with the Communist Party). Experts consider it to be a desirable information system practice to either remove from active files (purge) or to destroy dated information which may be misleading. *See, e.g.*, NATIONAL ADVISORY COMMISSION ON CRIMINAL JUSTICE STANDARDS AND GOALS, REPORT ON THE CRIMINAL JUSTICE SYSTEM 105-07 (1973) (recommended purging of criminal histories within 5 and 10 year periods depending upon seriousness of the crime).

agencies possessing the information do not establish adequate safeguards for preserving the confidentiality of the information.[114] Professor Charles Fried has written: "privacy is not just an absence of information abroad about ourselves; it is a feeling of security in control over that information."[115] In *Shelton v. Tucker*,[116] the Supreme Court cited lack of adequate security as a reason for holding unconstitutional a statute requring teachers to file with the appropriate hiring authority a list of every organization to which they belonged:

> The statute does not provide that the information it requires be kept confidential. Each school board is left free to deal with the information as it wishes. The record contains evidence to indicate that fear of public disclosure is neither theoretical nor groundless.[117]

Among necessary safeguards for preserving confidentiality would be regulations or legislation restricting access to information and providing appropriate sanctions against those officials who intentionally or negligently permit unauthorized access. It is even conceivable that in certain cases an individual may have a right to insist on certain minimum physical security procedures such as computer programming safeguards and restricted points of entry to areas where files are kept.[118]

3. *Improper Dissemination*

If rights of informational privacy may be infringed by improper collection and maintenance of personal information, obviously overly broad dissemination of such information would also constitute an infringement.[119] Improper dissemination may occur any time informa-

114. *See* Roe v. Ingraham, 480 F.2d 102, 108 (2d Cir. 1973); State v. Jacobus, 75 Misc. 2d 840, 846, 348 N.Y.S.2d 907, 913 (Sup. Ct. 1973).

115. Fried, *Privacy*, 77 YALE L.J. 475, 493 (1968).

116. 364 U.S. 479 (1960).

117. *Id.* at 486 (footnotes omitted).

118. *See, e.g.*, J. MARTIN & A. NORMAN, THE COMPUTERIZED SOCIETY 481-88 (1970), for a discussion of possible minimum safeguards.

119. The right to restrict dissemination of personal information may sooner or later collide with an emerging constitutional right of the public and press to have access to governmental information. *See generally* Note, *The Rights of the Public and the Press to Gather Information*, 87 HARV. L. REV. 1505 (1974). The right to informational privacy may also conflict with the statutory rights of access to personal information created under state or federal freedom of information acts. *See, e.g.*, Rose v. Department of Air Force, 495 F.2d 261, 267-68 (2d Cir. 1974) (Air Force Academy officials need not turn over case summaries of honor code violations to law review researchers without a prior in camera judicial inspection of the summaries for the purpose of insuring against a violation of privacy); Wine Hobby, USA, Inc. v. United States Bur. of Alcohol, 363 F. Supp. 231, 237 (E.D. Pa. 1973) (release of names of individuals permitted to produce wine for family use to a wine equipment distributor does not violate the constitutional right of privacy).

tion is transmitted to persons who do not possess a "need-to-know" related to a legitimate government function.[120] This is particularly true when information is transmitted for a private rather than a public purpose. The circulation by the police of an assault victim's nude photographs by police in *York v. Story*[121] provides a blatant example. Improper dissemination may also occur whenever the information is provided to persons who are likely to misuse the information either negligently or intentionally. The transmission of psychological records to untrained school personnel in *Merriken v. Cressman*[122] illustrates the problem.

It is likely that courts in the future will be confronted with objections to the dissemination of personal information from one government agency to another. In a recent case,[123] an individual sought damages for violation of his right to privacy as a result of a computer comparison of persons receiving veterans disability benefits with those receiving social security benefits. The plaintiff who received both types of payments incurred a drastic but lawful reduction in his disability pension as a result of the findings of the cross-comparison. The court held that no violation of the individual's right of privacy occurred, but also observed:

> What we have said *supra* is not intended to minimize the problems presented by the interagency transfer of information within the federal government. Nor do we suggest that a constitutional right of privacy might not be found to exist and appropriate relief granted in instances where the government is possessed of highly personal and confidential information which has been given under compulsion of law and with an expectation of privacy and where the disclosure of such information is unnecessary for the advancement or inconsistent with the fundamental purposes for which the data was obtained. Rather, we hold only that, on the facts of this case, Mr. Jaffess has not been deprived of any constitutionally secured privacy right.[124]

D. Fundamental Rights and Sensitive Information

In *Roe* v. *Wade*[125] the United States Supreme Court held that

120. See text accompanying notes 123-24 *infra*.

121. 324 F.2d 450 (9th Cir. 1963), *cert. denied*, 376 U.S. 939 (1964).

122. 364 F. Supp. 913 (E.D. Pa. 1973).

123. Jaffess v. Secretary, Dep't of Health, Ed. & Welf., 393 F. Supp. 626 (S.D.N.Y. 1975).

124. *Id.* at 629-30.

125. 410 U.S. 113, 152-56 (1973). In certain informational privacy decisions where the plaintiff has been successful, a fundamental rights test requiring a compelling state interest has been employed. City of Carmel-By-The Sea v. Young, 2 Cal. 3d 259, 268, 466 P.2d 225, 232, 85 Cal. Rptr. 1, 8 (1970); Eddy v. Moore, 5 Wash. App. 334, 345, 487 P.2d 211, 217 (1971). *See also* Roe v. Ingraham, 480 F.2d 102, 109 (2d Cir. 1973); Merriken v. Cressman, 364 F. Supp. 913, 918 (E.D. Pa. 1973); Davidson v. Dill, 180 Colo. 123, 131, 503 P.2d 157, 161 (1972). Other courts have not used the compel-

79-064 O - 76 - 77

privacy was a fundamental right requiring a compelling state interest to justify intrusion by the government. Justice Rehnquist, dissenting, declared that the Court's holding amounted to a return to substantive due process, a legitimation of judicial lawmaking.[126] The justice's concern is understandable. The fundamental rights doctrine is a potentially powerful tool for judicial intervention since it inevitably involves the conscious weighing of competing factors in a manner similar to that of a legislative body. It shifts the burden of persuasion from the individual to the government and requires legislatures to employ the least drastic means in achieving its objectives.[127] Originally forged in equal protection cases,[128] the doctrine was transplanted in *Roe* to the due process clause of the Fourteenth Amendment.[129] Concern over its potential scope influenced the Court in *San Antonio Independent School District v. Rodriguez*[130] to caution against overly broad interpretations:

> It is not the province of this Court to create substantive constitutional rights in the name of guaranteeing equal protection of the laws. Thus, the key to discovering whether education is "fundamental" is not to be found in comparisons of the relative societal significance of education as opposed to subsistence or housing. Nor is it to be found by weighing whether education is as important as the right to travel. Rather, the answer lies in assessing whether there is a right to education explicitly or implicitly guaranteed by the Constitution.[131]

Whatever the ultimate scope of the fundamental rights doctrine, *Roe* v. *Wade* assures its inevitable invocation whenever privacy interests are the subject of litigation. The prohibitions contained in the First, Fourth and Fifth Amendments indicate the high priority placed on limiting governmental informational gathering in the American political system.[132] A strong argument, therefore, can be made that the right to control highly personal information is a fundamental right implicitly guaranteed by the Constitution.

---

ling state interest test, although they have employed close judicial scrutiny of some kind. *See, e.g.*, United States v. Hudson, 103 Wash. Law Rptr. 377 (D.C. Super. Ct. 1975).

126. Roe v. Wade, 410 U.S. 113, 173-75 (1973).

127. *See, e.g.*, Shapiro v. Thompson, 394 U.S. 618, 637 (1969). The origins of the fundamental rights doctrine may be traced to Supreme Court decisions suggesting that stricter standards of review are appropriate where certain basic rights are involved. For example, in *Shelton v. Tucker*, 364 U.S. 479, 488 (1960), a case involving associational privacy, the Supreme Court declared: "In a series of decisions this Court has held that, even though the governmental purpose be legitimate and substantial, that purpose cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved."

128. *See, e.g.*, Shapiro v. Thompson, 394 U.S. 618 (1969).

129. Roe v. Wade, 410 U.S. 113, 153 (1973).

130. 411 U.S. 1 (1973).

131. *Id.* at 33-34.

132. See text accompanying notes 12-47 *supra*.

In precisely what situations should courts apply the fundamental rights test? There is little specific guidance from the Supreme Court on this question. One answer to this question would be to assume that privacy of whatever type is a fundamental right. Proceeding on this broad assumption could create severe practical problems. There are many areas where the collection and dissemination of information is useful to officials, but not necessarily justifiable by a compelling state interest. Should a police officer, for example, be required to demonstrate a compelling state interest when he asks the name and address of a person in the course of an investigation of a suspicious incident?[133]

A second approach would be to consider as fundamental only those informational privacy questions arising in areas which the court has already indicated are within the zone of general constitutional privacy—"the personal intimacies of the home, the family, marriage, motherhood, procreation, and child rearing."[134] The disadvantage to this approach is that it would likely exclude other types of information deserving an equally high level of protection, such as certain criminal justice and medical information.[135]

A third and perhaps the most preferable approach would be to recognize that *Roe* dealt with a matter—the decision to have an abortion—which many people would be reluctant to discuss even with their closest friends, let alone a public official. It may be that informational privacy rises to a fundamental right only whenever equally personal or sensitive matters are involved.[136]

While it is beyond the scope of this note to detail what information should be labeled sensitive, it is possible to suggest a general standard. Sensitive information is that which a person desires to keep private and which, if disseminated, would tend to cause substantial concern, anxiety or embarrassment to a reasonable person.[137] Although persons will

133. *See* Township of East Brunswick v. Malfitano, 108 N.J. Super. 244, 260 A.2d 863 (1970) (holding that the constitutional right of privacy does not justify a trespasser's refusal to answer a police inquiry concerning his name and address).

134. Paris Adult Theatre I v. Slaton, 413 U.S. 49, 65 (1973).

135. See text accompanying notes 48-77 *supra.*

136. Note, *Constitutional Right of Privacy and Investigative Consumer Reports: Little Brother Is Watching You*, 2 HAST. CONST. L.Q. 773, 792-97 (1975) (argument that the constitutional right of privacy protects against disclosure of "personal" information in credit reports).

137. *Cf.* W. PROSSER, LAW OF TORTS §§ 111, 117 (4th ed. 1971). The Supreme Court, of course, has already recognized the utility in distinguishing certain types of information from others. For example, in *Wisconsin v. Constantineau*, 400 U.S. 433, 437 (1971), the Court required a hearing where stigmatizing information is publicly disseminated. For those questioning the propriety of an objective standard, it should be noted that the Supreme Court has employed similar standards in resolving other constitutional issues. *See, e.g.*, Miller v. California, 413 U.S. 15 (1973); Katz v. United States, 389 U.S. 347 (1967).

differ on the meaning of sensitive, general classification according to the degree of sensitivity is not an impossible task. Presumably included within this standard would be information relating to those intimate matters already identified by the Supreme Court as coming within the zone of general constitutional privacy.[138] Also included as sensitive information would be certain types of medical, psychological and criminal justice information.[139] Excluded would be much of what has been earlier in this note labeled as administrative information,[140] such as the existence of a driver's license or a passport. Whether financial information would be considered sensitive should depend upon how complete and detailed was the statement of a person's economic affairs.[141]

The sensitivity of information would, therefore, determine whether challenged collection, maintenance or dissemination by public agencies would receive strict judicial scrutiny. If information is sensitive, the state should have to show that any infringements of individual rights concerning the information are necessary to promote a compelling governmental interest. If information is nonsensitive, a less restrictive standard of judicial scrutiny could be employed.

The practical effect of applying a compelling state interest test would be to shift the burden to the state to demonstrate that the collection was *essential* to further an interest which the government is constitutionally entitled to promote or protect.[142] But the burden of the state should not end there. It would also have the burden of demonstrating that the information was maintained in such a manner as to minimize the risk of unauthorized access,[143] and that any dissemination

138. See text accompanying notes 38-44 *supra.*

139. See text accompanying notes 48-71 *supra.*

140. See note 3 *supra.*

141. *Cf.* California Bankers Ass'n v. Shultz, 416 U.S. 21, 78 (1974) (Powell & Blackmun, JJ., concurring).

142. In First Amendment right of association cases where a compelling state interest test was employed, various phrases were used to emphasize the high degree of relevancy of disclosure of the information to a state interest. *See, e.g.*, Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539, 549 (1963) (must be "essential" or have a "crucial relation" to a governmental purpose); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 466 (1958) (must be a "controlling justification" for the disclosure).

143. See text accompanying note 114 *supra.* One authority lists six levels of potential protection which appear to be applicable to either manual or automated information systems:

1. Protection against accidental disclosure of secure information.
2. Protection from casual entry by unskilled persons.
3. Protection from casual entry by skilled technicians.
4. Protection against entry by persons who stand to gain financially.
5. Protection against well-equipped criminals.
6. Protection against organizations with massive funds.

J. MARTIN & A. NORMAN, THE COMPUTERIZED SOCIETY 481 (1970). Levels 1 through

was essential to further legitimate governmental functions. A criminal justice agency may, for example, find the retention of arrest records of acquitted persons necessary for the compilation of statistics on criminal careers, but if it disseminates the records to employers, or improperly maintains the records so that they are easily accessible to unauthorized persons, the subject's right of privacy may be violated.

In the case of non-sensitive information courts might turn to a more permissive standard—some type of reasonable relationship test.[144] Once a court was satisfied that the state's information-gathering practices—collection, maintenance, dissemination—were reasonably related to a legitimate governmental purpose, its inquiry would end. In other words, collection and dissemination of nonsensitive information which would directly assist in the furtherance of the public interest would be permissible. Even under this looser standard, however, minimum measures would have to be taken by the state to preserve the confidentiality of the information where public disclosure would not be necessary. The tendency of courts in applying the reasonable relationship test in other contexts has been to give only the scantest attention to the question of state interest.[145] Hopefully that would not happen in this area. Inquiry into whether government data processing activities actually further legitimate ends is possible without a usurpation of legislative functions.[146] Courts, need not, and should not, totally defer to unsupported assertions by officials concerning the value and integrity of their systems.

II. A Threshold Problem: The Case or Controversy Requirement

The Supreme Court has construed the case or controversy clause of Article III, section 2 to require that parties seeking relief in the federal courts must have sustained an injury or be in immediate danger of sustaining one.[147] Recent decisions of the Court raise the question of

---

5 could conceivably be considered as minimal levels of protection for sensitive data requiring fairly sophisticated system safeguards.

144. *See* Nebbia v. New York, 291 U.S. 502, 525 (1934); Note, *On Privacy*, *supra* note 44, at 772 n.660.

145. *See, e.g.*, Williamson v. Lee Optical, Inc., 348 U.S. 483 (1955).

146. The argument by Professor Gunther and others for stricter judicial scrutiny in areas not involving fundamental rights or suspect classifications may be adaptable to the area of informational privacy. Particularly interesting is Gunther's suggestion that courts should actively inquire into whether the government's means (in this case its information systems) *substantially* further legitimate ends. Gunther, *Forward: In Search of Evolving Doctrine on a Changing Court: A Model for Newer Equal Protection*, 86 HARV. L. REV. 1, 20-42 (1972). *See generally Forum: Equal Protection and the Burger Court*, 2 HAST. CONST. L.Q. 645 (1975). The difficulty with his suggestion, however, is that it may lead to precisely what the critics of substantive due process fear—an unwarranted intrusion into the province of the legislative branch.

147. California Bankers Ass'n v. Shultz, 416 U.S. 21, 56-57 (1974); Laird v. Tatum,

when the collection and dissemination of personal information by the government creates a threat of injury necessary to establish a constitutional case or controversy.[148] In partial answer to this question, the Court has drawn a distinction between situations where the government compels by summons or subpoena the reporting of certain information, and where it simply goes out and collects the information on its own.[149] Where the government requires self-reporting, the individual apparently has standing to contest disclosure.[150] It is in those cases where information is collected from persons or sources other than the individual to whom the information relates that difficulties may occur.

In *Laird* v. *Tatum*[151] the plaintiffs, political activists, sought a permanent injunction against the maintenance of an intelligence gathering system by the United States Army. The information was gathered by army "'surveillance of lawful and peaceful civilian political activity.'"[152] It "consisted essentially of . . . information about public activities that were thought to have at least some potential for civil disorder . . . ."[153] The principal sources for the information were the news media and publications of general circulation. The information gathered typically contained such data as the identity of speakers, numbers of people in attendance and whether a public disorder occurred. The information was disseminated to various army posts around the country.

The plaintiffs claimed that the recording of their political activities by army agents had a chilling effect on their First Amendment rights. A majority of the United States Supreme Court, unable to see a connection between the mere existence of the system and the alleged chilling effect, held that there was no justiciable controversy. According to the majority opinion, "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm . . . ."[154]

---

408 U.S. 1, 13-14 (1972). The requirement of injury is one of several distinct elements needed to establish standing in the federal courts. Note, *Recent Standing Cases and a Possible Alternative Approach*, 27 HASTINGS L.J. 213 (1975).

148. California Bankers Ass'n v. Shultz, 416 U.S. 21 (1974); Laird v. Tatum, 408 U.S. 1 (1972).

149. California Bankers Ass'n v. Shultz, 416 U.S. 21, 55-56 (1974); *see also* Shelton v. Tucker, 364 U.S. 479 (1960).

150. *See* California Bankers Ass'n v. Shultz, 416 U.S. 21, 55-56 (1974).

151. 408 U.S. 1 (1972).

152. *Id.* at 2.

153. *Id.* at 6. Although the majority opinion by Chief Justice Burger discusses no wider dissemination than within the United States Army, in his dissent Justice Douglas asserts that the information was disseminated to various federal agencies and local police departments. *Id.* at 26-27 (Douglas & Marshall, JJ., dissenting).

154. *Id.* at 13-14; *accord*, Davis v. Ichord, 442 F.2d 1207 (D.C. Cir. 1970).

Although decided more than a week after the burglary of the Democratic Party's national headquarters by members of President Nixon's campaign staff, *Laird* remains essentially a pre-Watergate decision. The Court's opinion exhibits an insensitivity to the dangers of unregulated intelligence gathering which might not have been present had the case been decided one or two years later. As Justice Douglas stated in his dissent: "[t]o withhold standing to sue until [one's job is lost] would in practical effect immunize from judicial scrutiny all surveillance activities, regardless of their misuse and their deterrent effect."[155]

Arguably *Laird* is still sound authority for the proposition that the mere compilation and dissemination of data which is publicly available does not pose a severe enough threat to an individual's First Amendment rights to create a justiciable chill. But the *Laird* Court was not faced with a challenge to the collection of highly personal information. In such cases the risk of harm to the subject of the information is appreciably greater.

Laird v. *Tatum* was followed by *California Bankers Association* v. *Shultz*,[156] a case challenging the constitutionality of a federal statute requiring the reporting and maintenance of financial information. The plaintiffs included banks, individual bank customers, the California Bankers Association and the American Civil Liberties Union (ACLU). Specifically, the statute and its implementing regulations required financial institutions to maintain records of customer transactions in excess of $100.[157] The ACLU challenged this requirement on the ground that such recordkeeping threatened the First Amendment rights of its members by exposing the identities of its members and contributors to possible identification by the government. The Court was not receptive. In a six-to-three opinion, it rejected the ACLU claim observing that the records were not in the hands of the government and that the government had made no attempt to compel production of such records.[158] The threat to First Amendment rights, the Court observed, was much less than that presented by the army's intelligence system in *Laird* v. *Tatum*.[159] The statute and the implementing regulations also required banks to report directly to the secretary of the treasury any domestic currency transactions in excess of $10,000.[160] In addition, individuals involved in foreign transactions of over $5,000 were required to report

155. Laird v. Tatum, 408 U.S. 1, 26 (1972) (Douglas & Marshall, JJ., dissenting).

156. 416 U.S. 21 (1974); Note, *California Bankers Ass'n v. Shultz: An Attack on the Bank Secrecy Act*, 2 HAST. CONST. L.Q. 203 (1975); *see also* notes 91-94 *supra*.

157. California Bankers Ass'n v. Shultz, 416 U.S. 21, 32 (1974).

158. *Id.* at 55-57.

159. *Id.* at 56-57.

160. *Id.* at 39.

similar information themselves.[161] The Court sidestepped depositor's challenges to these requirements by noting that they had not shown that they actually engaged in transactions which would be required to be reported.[162] Consequently, the Court concluded that the depositors had not presented a concrete controversy for adjudication.[163] By so holding, the Court appears to require, as an element of standing, specific allegations demonstrating that the government possesses, or will possess, information relating to the plaintiff.

A. The View from the Lower Courts

Admittedly, one possible interpretation of the Supreme Court's decisions in *Laird* and *California Bankers* is that regardless of who is holding information or what the nature of the information is, its mere collection is not sufficient to create a justiciable case or controversy.

Support for this exceedingly broad interpretation is found in a federal court of appeals decision, *Finley v. Hampton*.[164] In *Finley* a government employee brought an action against members of the Civil Service Commission and the secretary of the Department of Health, Education and Welfare to have expunged from his personnel file a statement that "two of his associates had 'homosexual mannerisms.' "[165] The employee could not show that he had suffered any pay or grade impairment as a result of the information, although his job was reclassified as nonsensitive following the collection of the information. Citing *Laird* v. *Tatum* as authority, the court held that there was no justiciable controversy because no threat of specific future harm resulted from the file's existence. The court noted that allegations of a subjective chilling effect on First Amendment rights of association were not an adequate substitute for "threat[s] of specific future harm."[166] *Finley* represents a significant extension of the case or controversy limitation. Unlike *Laird* or *California Bankers*, the information involved was highly personal containing not only a distinct chilling effect on First Amendment rights of association but also a threat to personal privacy. The information was not in the hands of a private agency such as a bank with a profit incentive to keep it confidential, nor in the hands of a government agency with no legal ability to apply sanctions or rewards to the subject of the file; instead the information was contained in the personnel file of the agency employing the plaintiff.

161. *Id.* at 35.
162. *Id.* at 68, 76.
163. *Id.*
164. 473 F.2d 180 (D.C. Cir. 1972).
165. *Id.* at 182.
166. *Id.* at 185.

Curiously, the same court ruled to the contrary two years later in *Menard v. Saxbe*,[167] a case involving arrest records. The plaintiff in that case had been arrested for burglary and subsequently released by the Los Angeles Police Department. The record of his arrest and his fingerprints were forwarded to the Federal Bureau of Investigation. Menard brought an action to have the arrest record maintained by the FBI expunged. The court of appeal held that Menard had standing to sue, stating that although, "Menard cannot point with mathematical certainty to the exact consequences of his criminal file, we think it clear that he has alleged a 'cognizable legal injury.' "[168]

Is there a logical, factual distinction to be made between the *Menard* and *Finley* decisions—between an arrest record and a personnel record implying that an employee is a homosexual? The answer lies in the original question articulated in *Laird* v. *Tatum*: is there a "claim of specific present objective harm or a threat of specific future harm?"[169] The threat of specific future harm would seem to be as great, if not greater, from the personnel record as from the arrest record. Certainly it can be argued that the adverse economic and psychological consequences are likely to be similar in nature. Yet the court made no attempt to reconcile the *Menard* and *Finley* decisions.

B. Defining a Cognizable Legal Injury

In discussing what constitutes a cognizable legal injury or harm courts have emphasized an identifiable loss (either actual or imminent) of tangible benefits. Courts have found no difficulty in finding a constitutional case or controversy where a person loses a job or some other equivalent benefit as the result of the dissemination of personal information.[170] Similarly, any public disclosure of personal information injurious to one's reputation is likely to provide the subject of the information with standing.[171] But there is a practical problem with limiting the definition of harm to situations where the effect of the information can be directly traced. Once potentially damaging information is in the hands of government officials, it may result in decisions of which the subject may never have knowledge.[172] It is impossible for

167. 498 F.2d 1017 (D.C. Cir. 1974).

168. *Id.* at 1023; *see also* Paton v. LaPrade, D.C. Civil No. 1091-73 (3d Cir., October 14, 1975).

169. Laird v. Tatum, 408 U.S. 1, 14 (1972).

170. *Id.* at 11-12. *See also* Socialist Workers Party v. Attorney General, 419 U.S. 1314 (Marshall, Cir. J., 1974); Handschu v. Special Services Division, 349 F. Supp. 766 (S.D.N.Y. 1972).

171. Philadelphia Yrly. Meet Rel. Society of Friends v. Tate, 519 F.2d 1335 (3d Cir. 1975) (disclosure by city officials over national television that plaintiff was the subject of a police intelligence file is actionable).

172. In one case, a New York Port Authority police detective was observed partici-

an individual to monitor all of the uses of personal information in the hands of public officials.

> On a given person there may be upwards of 100 files maintained in various organizations. These range in visibility from those in which data gathering, use and sharing goes on completely behind closed doors (*e.g.*, intelligence files) to those in which the individual has some knowledge about content and use but little, if any, knowledge about the data sharing which goes on from his file (as in the case of a bank which routinely shares its account experience information with credit bureaus).[173]

When consideration is given to the secondary and tertiary uses of personal information systems, the need for a flexibile definition of harm is easily recognized. The simplest path for the courts to take would be to declare that there is a threat of immediate harm any time public officials possess information which an individual has sought to keep reasonably private. Neither *Laird* nor *California Bankers Assocation* would necessarily bar such an approach. Its utility is readily apparent. It would permit challenges to information before any adverse social or economic consequences could flow from its use or disclosure. The individual need not identify or trace actual adverse effects resulting from the dissemination and use of the information. As a practical matter, however, any extensive broadening of the definition of harm might not be acceptable to the present Court with its rather narrow view on the question of standing.[174] Fear of frivolous suits by a conservative judiciary would pose a significant obstacle to a more permissive definition.

As a second alternative, therefore, plaintiffs in appropriate situations might attempt to employ the distinction between sensitive and nonsensitive information discussed earlier.[175] The distinguishing characteristic of sensitive information as defined in the note is that its public dissemination would tend to cause substantial concern, anxiety or embarrassment to a reasonable person.[176] This characteristic alone raises the threat of harm to a legally cognizable level. The mere fact of collection of sensitive information may involve an inhibiting effect on personal creativity and spontaneity, and create personal anxiety. Legally cognizable harm should be presumed to exist any time sensitive

---

pating in picketing out of uniform for higher wages. Despite a satisfactory employment rating, one of his superiors placed a comment in his personnel file indicating that the detective was an irresponsible commander. When the detective retired a few years later, he experienced serious difficulty in obtaining employment because his file had been widely circulated outside the Port Authority. J. RAINES, ATTACK ON PRIVACY 15 (1974).

173. Baker, *Record Privacy as a Marginal Problem: The Limits of Consciousness and Concern*, 4 COLUM. HUMAN RIGHTS L. REV. 89, 92 (1972).

174. *See generally* Note, *Recent Standing Cases and a Possible Alternative Approach*, 27 HASTINGS L.J. 213 (1975).

175. See text accompanying notes 137-41 *supra*.

176. See text accompanying notes 7-9 *supra*.

information is collected by public officials, unless it has been already voluntarily disseminated to the public by the person to whom it refers. The above test would avoid such patently unjust results as found in *Finley v. Hampton.*[177] Yet it also presents a compromise to those on the Court who express concern over a highly liberalized standing policy.

III. Conclusion

Several key generalizations have been emphasized in various portions of this note. First, although the overlap is inevitable, the right of informational privacy is analytically separate from other constitutionally recognized privacy rights. Second, the potential for infringment upon an individual's informational right of privacy exists whenever the government collects, maintains or disseminates information. Third, whether informational privacy is elevated to a fundamental right depends primarily upon whether the information in question is considered sensitive. Fourth, an individual's standing to enforce his right in federal courts requires a flexible definition of the harm needed to establish a justiciable case or controversy.

The informational privacy issues raised in this note are not likely to be resolved quickly or easily. As the problems of an urbanized America assume new dimensions, the demands for detailed personal information are likely to increase. For the purpose of meeting these demands, the physical, behavioral and biological sciences are developing new techniques to gather, process, classify and transmit highly sensitive data.[178] It would be reassuring to know as we move to a post-industrial society that we have not left basic constitutional principles behind.

---

177. 473 F.2d 180 (D.C. Cir. 1972). *See also* text accompanying notes 164-66 *supra.* An alternative approach may be suits in state courts. Plaintiffs in states having less restrictive doctrines of standing may be able to circumvent federal standing requirements by making their claims in state courts. *See* White v. Davis, 13 Cal. 3d 757, 533 P.2d 222, 120 Cal. Rptr. 94 (1975).

178. *See, e.g.,* Ausubel, Beckwith & Janssen, *The Politics of Genetics Engineering: Who Decides Who's Defective?,* 8 PSYCHOLOGY TODAY 30, 38 (June 1974) (reporting proposal by certain public officials that males with specific "criminal" chromosomes be registered at birth); Wilson, *Computerization of Welfare Recipients: Implications for the Individual and the Right to Privacy,* 4 RUTGERS J. COMPUTERS & L. 163, 165 (1974) (trend toward computerized welfare data banks on city-wide and regional basis); San Francisco Sunday Examiner & Chronicle, Nov. 9, 1975, § A, at 21, col. 1 (controversy over mental health screening accompanying free medical test given to poor families).

ELECTRONIC VISUAL SURVEILLANCE AND THE FOURTH AMENDMENT: THE ARRIVAL OF BIG BROTHER?

*By David P. Hodges**

I. Introduction

On February 8, 1974, Paul Castellano was holding a meeting in his office with three business associates. Apparently suspecting the group of involvement in organized crime, agents of the Federal Bureau of Investigation were using a hidden listening device to monitor the meeting and were also watching the group's activities by means of a television camera which they had secretly installed in the office. During the meeting Castellano suddenly discovered the listening device. As the agents watched on their television monitor, the men conducted a thorough search for other devices. The agents' view ended abruptly when the camera was discovered and smashed. Shortly thereafter, the agents entered the office. Unable to find the listening device, they arrested the four men for theft of government owned property.[1]

In an editorial referring to this incident, the *New York Times* commented that "it is an Orwellian act of official arrogance to assign inviolable status as government property to the instruments of clandestine intrusion on a citizen's office or home,"[2] and asked: "Must the target of a wiretap adjust to the bug as constant companion? Is it a must to stay on camera?"[3] The editorial conceded, however, that "presumably the equipment was installed by the F.B.I. with court sanction."[4] The latter comment provides the focus for this note: May a court constitutionally authorize the installation of clandestine electronic visual surveillance devices for law enforcement purposes?

A carefully circumscribed statutory procedure has been established under which wiretapping and electronic eavesdropping are permitted for law enforcement purposes when conducted in accordance with prior

---

* Member, second year class.

1. N.Y. Times, Feb. 12, 1974, at 35, col. 1.
2. N.Y. Times, Feb. 13, 1974, at 38, col. 1.
3. *Id.*
4. *Id.*

judicial authorization.[5] The listening device installed in Mr. Castellano's office, if authorized and operated in the manner prescribed by this statute, was therefore a constitutionally permissible investigative tool.[6] However, the statute does not apply to the use of a hidden camera to spy on the activities of individuals,[7] nor has the Supreme Court ever considered the constitutionality of the use of such a device.[8] Nevertheless, the Castellano incident illustrates that "electronic snooping"[9] is now emerging as a tool of law enforcement. This development raises some serious constitutional questions involving the conflict between the legitimate need of society for effective law enforcement and the right of the individual members of society to be free from unreasonable governmental intrusions.[10]

The individual's "right of privacy" is a cherished value of American society. Yet the meaning of privacy varies depending on the factual context and the expectations of the individual concerned. Privacy has been defined, for example, as the right "to be let alone,"[11] the right of persons "to determine for themselves when, how, and to what extent information about them is communicated to others,"[12] and as the right

5. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520 (1970) [hereinafter referred to in text and notes as Title III]. See notes 107-116 *infra* and text accompanying.

6. The constitutionality of Title III has not been directly considered by the Supreme Court, but has been upheld by all of the federal courts of appeals that have considered the issue. *See, e.g.*, United States v. Sklaroff, 506 F.2d 837 (5th Cir.), *cert. denied*, 96 S. Ct. 142 (1975), and cases cited therein at 840.

7. Title III applies only to the "*aural* acquisition of the contents of any wire or oral communication . . . ." 18 U.S.C. § 2510(4) (1970) (emphasis added). *See* S. REP. No. 1097, 90th Cong., 2d Sess. 90 (1968) [hereinafter cited as SENATE REPORT] (other forms of surveillance not within the proposed legislation).

8. Research has revealed only one case that mentions the use of a hidden camera by law enforcement agents. In Sponick v. Police Dep't, 49 Mich. App. 162, 211 N.W.2d 674 (1973), F.B.I. agents concealed a camera in the wall of a bar to watch for suspected gambling activity. Since the bar was a public place, the court held that the use of the camera was not a search under the Fourth Amendment. *Id.* at 198, 211 N.W.2d at 690. See notes 69-75 *infra* and text accompanying.

9. The use of electronic devices for the purpose of visual surveillance will hereinafter be referred to as "electronic snooping," as distinguished from the use of electronic devices for the purpose of aural surveillance (including both wiretapping and bugging), which will hereinafter be referred to as "electronic eavesdropping." The term "electronic surveillance" will refer to both of these and to any other electronic methods for clandestine surveillance of persons. *See, e.g.*, United States v. Holmes, 521 F.2d 859 (5th Cir. 1975) ("beeper" attached to car for constant surveillance of car's location); United States v. Martyniuk, 395 F. Supp. 42 (D. Or. 1975) (same).

10. *See* Terry v. Ohio, 392 U.S. 1, 10-12 (1968); Camara v. Municipal Court, 387 U.S. 523, 528, 533 (1967); Frank v. Maryland, 359 U.S. 360, 363-65 (1959).

11. Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890).

12. A. WESTIN, PRIVACY AND FREEDOM 7 (1967) [hereinafter cited as WESTIN].

which protects "the individual's interest in preserving his essential dignity as a human being."[13] The Supreme Court has held that there is a constitutional right of privacy which absolutely prohibits governmental interference in certain areas of individual activity.[14] But the Fourth Amendment contains no general right to privacy absolutely prohibiting governmental intrusion;[15] rather, it protects only against "unreasonable" governmental intrusions.[16] The primary constitutional question posed by electronic snooping is whether there are circumstances under which the invasion of privacy which it entails can be considered reasonable and thus permissible under the Fourth Amendment.

The question of the protection of individual privacy has come into sharper focus since the elctronic age has expanded the means by which searches and seizures may be accomplished. The drafters of the Fourth Amendment were concerned only with the permissible scope of a physical entry into a person's home or business and the seizure of physical objects. That "zone of privacy" which protected spoken words from overhearing and acts from observation was fixed by the inherent limits of the human senses. Privacy against prying eyes and ears could be insured when such privacy was desired. The advent of electronics, however, has eliminated the traditional zone of privacy with respect to one's spoken words since eavesdropping devices can detect what is said virtually anywhere.

Members of the Supreme Court, recognizing the impact on traditional notions of privacy of the "frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society,"[17] have long expressed their apprehension over the predictable improvements in sophistication of such devices. In his famous dissent in the first wiretapping case considered by the Court, Justice Brandeis warned that "[t]he progress of science in furnishing the Government with

13. Hufstedler, *The Directions and Misdirections of a Constitutional Right of Privacy*, 26 RECORD OF N.Y.C.B.A. 546, 550 (1971) [hereinafter cited as Hufstedler]. *See generally* Fried, *Privacy*, 77 YALE L.J. 475 (1968).

14. *E.g.*, Roe v. Wade, 410 U.S. 113 (1973) (individual decision to have an abortion); Stanley v. Georgia, 394 U.S. 557 (1969) (possession of obscene materials in the home); Griswold v. Connecticut, 381 U.S. 479 (1965) (use of contraceptives by married persons). A similar right has been recognized by state courts. *E.g.*, State v. Bateman, 25 Ariz. App. 1, 540 P.2d 732 (1975) (consenting sexual behavior by a married couple in private); Ravin v. State, 537 P.2d 494 (Alas. 1975) (possession of marijuana for personal use in the home).

15. Katz v. United States, 389 U.S. 347, 350 (1967).

16. Carroll v. United States, 267 U.S. 132, 147 (1925).

17. Silverman v. United States, 365 U.S. 505, 509 (1961).

means of espionage is not likely to stop with wire-tapping."[18] Justice Murphy foresaw that "new methods of photography that penetrate walls or overcome distances" would be "far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears . . . ."[19] Chief Justice Warren referred to the danger posed by "the fantastic advances in the field of electronic communication . . . ."[20] Justice Douglas expressed his concern that "[w]e are rapidly entering the age of no privacy, where everyone is open to surveillance at all times . . . ."[21]

These apprehensions have been realized by the development of electronic snooping devices, which now threaten to eliminate the barrier against visual intrusion upon an individual's traditional zone of privacy. The implications of electronic snooping are far more serious than those of electronic eavesdropping.[22] For this reason it is imperative that electronic snooping not be considered merely an extension of electronic eavesdropping, to be utilized in law enforcement subject to no greater constitutional or statutory restrictions. As an inherently more intrusive surveillance technique, electronic snooping must be separately evaluated against the constitutionally mandated standard of reasonableness.

Compelling reasons require that the legal community address this issue *now*, before the official use of electronic snooping becomes widespread. A time delay invariably exists between the introduction of a new technology and judicial consideration of its constitutional implications.[23] Recent technological progress, particularly in the field of electronics, has resulted in "a drastic acceleration of the process of innovation, invention and practical application of new technology."[24] Consequently this time delay has taken on increased significance where new

18. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

19. Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting).

20. Lopez v. United States, 373 U.S. 427, 441 (1963) (Warren, C.J., concurring in the result).

21. Osborn v. United States, 385 U.S. 323, 341 (1966) (Douglas, J., dissenting).

22. "When—and this may be in the not-too-distant future—walls cease to be a barrier to visual aids, it will be the visual eavesdropper who poses the greatest threat to the right of privacy." Comment, *Electronic Eavesdropping: A New Approach*, 52 CALIF. L. REV. 142, 147 (1964).

23. *See generally* Green, *The New Technological Era: A View From the Law*, BULL. OF THE ATOMIC SCIENTISTS, Nov. 1967, at 12.

24. Green, *Technology Assessment and the Law: Introduction and Perspective*, 36 GEO. WASH. L. REV. 1033, 1034 (1968). For specific examples, see references cited in note 34 *infra*.

electronic surveillance techniques are concerned.[25] By the time Congress acted to bring electronic eavesdropping under statutory control, the technology had been in widespread use for many years.[26] A total ban on electronic eavesdropping, although proposed,[27] would have been unrealistic and probably unworkable under the circumstances.

Electronic snooping, on the other hand, is not yet in widespread use. Effective regulation of its use in law enforcement is therefore possible. Now is the critical time to ask whether the use of electronic snooping as a law enforcement tool should be permitted under any circumstances. This note will examine the constitutionality of electronic snooping techniques which intrude upon an individual's "reasonable expectation of privacy"[28] protected by the Fourth Amendment to the Constitution. The discussion will proceed by analogy to the constitutional principles relating to electronic eavesdropping,[29] taking into account relevant differences between the two techniques. It is appropriate to begin this inquiry with an examination of the exact nature of the technology of electronic snooping and its present and future capabilities.

---

25. "Technological developments are arriving so rapidly and are changing the nature of our society so fundamentally that we are in danger of losing the capacity to shape our own destiny.

"This danger is particularly ominous when the new technology is designed for surveillance purposes, for in this case the tight relationship between technology and power is most obvious. Control over the technology of surveillance conveys effective control over our privacy, our freedom and our dignity—in short, control over the most meaningful aspects of our lives as free human beings." *Hearings on Surveillance Technology Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 95th Cong., 1st Sess., June 23, 1975 (opening statement of Senator Tunney) (mimeographed copy obtained from Senator Tunney's office). "The law, though jealous of individual privacy, has not kept pace with [the] advances in scientific knowledge." Berger v. New York, 388 U.S. 41, 49 (1967). "[O]ur course of decisions, it now seems, has been outflanked by the technological advances of the very recent past." Lopez v. United States, 373 U.S. 427, 471 (1963) (Brennan, J., dissenting).

26. *See* Berger v. New York, 388 U.S. 41, 45-47 (1967).

27. S. 928, 90th Cong., 1st Sess. (1967) (Right of Privacy Act of 1967). *See generally* SENATE REPORT, *supra* note 7, at 161-62 (individual views of Senator Long and Senator Hart).

28. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). See notes 69-75 *infra* and text accompanying.

29. Electronic snooping is more closely analogous to electronic eavesdropping than to an ordinary physical entry because it involves the same electronic extension of the unaided senses, the same lack of presearch notice, and normally the same kind of search for evidence from the acts of the suspect himself rather than from the seizure of a specific tangible object which may be found in the place searched. But see note 125 *infra* and text accompanying. Thus the constitutional issues raised by electronic snooping are most logically approached by analogy to the law relating to electronic eavesdropping.

II. The Tools

A. Miniature Television Cameras

The potential usefulness of hidden television cameras to view areas otherwise inaccessible to unaided visual perception has long been recognized.[30] Writers have described visual surveillance systems consisting of cameras installed between walls and fitted with a ninety-degree mirror to observe the adjoining room,[31] mounted on a telephone pole to look into apartment windows across the street,[32] and placed in the ventilators of public restrooms to detect and apprehend homosexuals.[33] But these systems have not been widely used for visual surveillance of private areas since they generally lacked portability and were difficult to install, conceal and maintain.

These problems have been virtually eliminated by the introduction of cameras equipped with a very recently developed solid-state image sensor called a "charge-coupled device" (CCD).[34] Currently about the size of a nickel, the CCD replaces the bulky and expensive tubes which were previously the heart of a television camera. The development of the first complete closed-circuit camera system using CCD technology was announced in 1973.[35] The camera was hand-held, measured three inches by two inches by one inch and weighed six ounces. Only one month later a considerably more sophisticated sensor was unveiled,[36] and early in 1975 a camera became available which incor-

30. *See, e.g.*, WESTIN, *supra* note 12, at 71-72; S. DASH, R. SCHWARTZ, & R. KNOWLTON, THE EAVESDROPPERS 375-78 (1959) [hereinafter cited as DASH].

31. Sanford, *TV for Surveillance*, LAW AND ORDER, Dec. 1964, at 16.

32. Shaw, *An Introduction to Law Enforcement Electronics and Communications, Part III*, LAW AND ORDER, May 1965, at 36.

33. WESTIN, *supra* note 12, at 131.

34. *See generally* Amelio, *Charge-Coupled Devices*, SCIENTIFIC AMERICAN, Feb. 1974, at 22; Gilmore, *Tiny TV Camera With a Big Future*, POPULAR SCI., Aug. 1972, at 28. The CCD is the latest product of the burgeoning semiconductor electronics industry, which, although less than thirty years old, has already had a remarkable impact on society. For a glimpse of the speed with which the industry is inventing and improving new electronic devices, *compare* Vacroux, *Microcomputers*, SCIENTIFIC AMERICAN, May 1975, at 32, *with* Hittinger & Sparks, *Microelectronics*, SCIENTIFIC AMERICAN, Nov. 1965, at 57. CCD technology may similarly be expected to undergo rapid development, leading to greatly improved sophistication and further reduction in size.

35. N.Y. Times, Aug. 22, 1973, at 54, col. 1; BUS. WEEK, Aug. 25, 1973, at 21.

36. N.Y. Times, Sept. 19, 1973, at 68, col. 4. "Sophistication" in this sense refers to the sensor's resolution, image quality, and light-gathering efficiency, which are dependent upon the number of independent "elements" (literally, "eyes") contained in each sensor. The original CCD contained 10,000 elements; the later device contained 120,000. The rapid improvement typical of new semiconductor devices is thus strikingly illustrated.

79-064 O - 76 - 78

porated this sensor and was fully compatible with existing television monitors, videotape recorders and other equipment.[37]

Such miniaturized cameras can easily be concealed in a briefcase, a kitchen cabinet, a lamp base, a room heating duct, an overhead lighting fixture or even in an electrical outlet or light switch. One writer has predicted the development of wireless, battery-powered electronic "eyes" as small as buttons.[38] This prospect seems assured with the advent of CCD technology. Thus the capability currently exists to gain visual access to virtually any private area, in a manner similar to the use of miniature listening devices to overhear private conversations.[39]

B. Light Pipes

Another recent development which can be utilized in conjunction with miniature television cameras is the technology of "fiber optics."[40] This technology employs a small bundle of thin, transparent and flexible fibers called a "light pipe" which can conduct light or visual images from one end of the bundle to the other even when the fibers are twisted or completely coiled up. At one end of the pipe is a lens and at the other a television camera, which can be located at a convenient distance from the area under surveillance. Only the lens need actually intrude into the target area, and its presence can be easily concealed. There are few places into which an expertly installed light pipe cannot intrude. Any installation difficulties attending the use of television cameras for surveillance would thus be eliminated.

C. Low Light Level Television

Another facet of a comprehensive electronic snooping system is the ability to virtually "see in the dark." One means by which this may be accomplished is through the technology of Low Light Level Television (LLLTV),[41] which utilizes an extremely sensitive visual detector. An

37. N.Y. Times, Jan. 28, 1975, at 48, col. 4.

38. WESTIN, *supra* note 12, at 86.

39. *See generally* DASH, *supra* note 30, at 330-58. One difference between visual and aural "bugs," of course, is that the visual device must be in plain sight in the area under surveillance. Nevertheless, appropriate camouflage techniques can be employed to minimize the risk of inadvertent detection.

40. *See generally* Goldberg, *Fiber Optics*, POPULAR PHOTOGRAPHY, Nov. 1971, at 100.

41. *See generally* Norwood, *"Available Dark" Photography*, INDUSTRIAL PHOTOGRAPHY, Nov. 1971, at 24 (describing the development of LLLTV technology for use in Vietnam, and its conversion to domestic law enforcement purposes upon declassification of information about the system).

area which appears dark to the naked eye can be viewed on a television screen as if in bright daylight by the use of such systems. Under grants from the Law Enforcement Assistance Administration, LLLTV systems have been installed in several cities to provide remote surveillance of downtown business areas in an effort to reduce street crime and better utilize police resources.[42] With the development of charge-coupled devices incorporating low light level capabilities,[43] electronic snooping systems can now provide surveillance of enclosed areas under any conceivable lighting conditions. No longer is darkness a barrier to an electronic snooper.

D. Infrared Television Cameras

Another method of "seeing in the dark" involves the use of devices which detect infrared radiation.[44] Originally developed for night vision use by the military, these devices now have been adapted for civilian purposes.[45] The earlier models utilized the "direct viewing" system, in which invisible infrared radiation illuminates the area under observation and the reflections are detected by a television camera sensitive to such radiation, just as visible radiation is detected by an ordinary camera.[46] A more sophisticated method uses the "thermal imaging" system, which directly detects infrared radiation and converts it into electrical energy.[47] By discriminating between the minute differences in temperature of various parts of the body, this system can produce a high-resolution black and white television image of a person, including all facial details, at a distance of several hundred yards, even on an overcast night or through dense fog.

Although these infrared sensors can be used in miniature television cameras as an alternative to the LLLTV technique, the most signficant

42. *See generally* Donner, *Political Intelligence: Cameras, Informers, and Files*, 1 CIV. LIB. REV. 8, 13 (1974); Note, *Police Use of Remote Camera Systems for Surveillance of Public Streets*, 4 COLUM. HUMAN RIGHTS L. REV. 143-53 (1972).

43. *See generally* Carnes & Kosonocky, *Sensitivity and Resolution of Charge-Coupled Imagers at Low Light Levels*, 33 RCA REV. 607 (1972).

44. Infrared radiation may be more familiarly described as heat. For example, because of its warmth the human body emits infrared radiation. Although not visible to the human eye, such radiation can be detected by appropriate electronic devices.

45. *See, e.g.*, THE ENGINEER, July 5, 1973, at 23 (describing an infrared surveillance system for security against intruders).

46. *See* Swift & Thompson, *Seeing in the Dark*, 42 THE RADIO AND ELECTRONIC ENGINEER 403 (1972). A drawback of this system was that if the person being observed also possessed an infrared detector he could detect the presence of the viewer and guard against it.

47. *See id.* at 408.

feature of infrared technology is that eventually it may provide a means to literally see through walls. Most present building materials, such as wood and brick, are as opaque to infrared radiation as they are to visible light. However, certain substances in widespread use, such as plastics, are excellent transmitters of infrared energy even when painted and thus opaque to visible light.[48] To a lesser extent glass and derivative materials such as fiberglass also transmit infrared radiation. The day may soon arrive when the infrared emanations from a human body, passing through the four walls which have traditionally afforded privacy from visual intrusions, can be detected and reconstructed into a television picture by a nearby snooper. Such a development would remove the last barrier to unwanted visual observation of private areas.

E. Videophones

One other means of visual intrusion, the videophone, deserves brief attention. The videophone is an ordinary telephone incorporating a television camera and viewing screen which permit the parties to a conversation to see each other while they talk. Although their development has not been as rapid as originally predicted,[49] videophones may eventually become commonplace in private homes and businesses.[50] In a manner analogous to present methods of wiretapping,[51] an electronic snooper equipped with a television monitor could intercept both the visual images and the oral communications of the parties to a videophone conversation.[52]

III. Is Electronic Snooping A Search?

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

---

48. *Cf.* WESTIN, *supra* note 12, at 71 (describing wall panels made of a special substance which transmits infrared).

49. *See* Hardeman, *When Will Picturephone Break Out?*, ELECTRONICS, Nov. 8, 1971, at 97.

50. A major step toward the mass production of a low cost, reliable videophone may be the recent development of a CCD for use in videophones. *See* N.Y. Times, Jan. 4, 1975, at 29, col. 4.

51. *See generally* DASH, *supra* note 30, at 306-30.

52. Interception of the visual portion of the communication is not presently prohibited. See note 7 *supra*.

In determining the applicability of the Fourth Amendment to a particular type of official conduct, two questions must be considered:

1. Does the conduct constitute a search or seizure within the meaning of the amendment?
2. Is the conduct unreasonable?[53]

Only if both of these questions are answered in the affirmative will the conduct constitute a violation of the Fourth Amendment.[54]

A. The Original Trespass Doctrine

The Supreme Court long ago declared that the protection of the Fourth Amendment applies "to all invasions on the part of the government and its employés of the sanctity of a man's home and the privacies of life."[55] Notwithstanding the breadth of this language, the terms "search" and "seizure" were originally limited to an actual physical trespass into a person's dwelling or place of business and to the seizure of tangible objects.[56] With the increasingly prevalent use of electronic eavesdropping, however, came the realization that wiretapping and bugging intruded upon the privacies of life protected by the Fourth Amendment just as effectively as did the more traditional physical entry into the home. When an actual physical trespass occurred, the Court was quick to find a Fourth Amendment violation even though only conversations had been "seized."[57] The Court soon explicitly held that conversation, although an intangible, could be the subject of Fourth Amendment

53. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 16-20 (1968); Boyd v. United States, 116 U.S. 616, 621-22 (1886).

54. The consequence of a Fourth Amendment violation is that no evidence thus obtained is admissible in a state or federal criminal prosecution. Mapp v. Ohio, 367 U.S. 643 (1961) (state prosecution); Weeks v. United States, 232 U.S. 383 (1914) (federal prosecution). *But see* United States v. Peltier, 422 U.S. 531 (1975) (extension of exclusionary rule not retroactively applied); United States v. Calandra, 414 U.S. 338 (1974) (refusing to extend the exclusionary rule to grand jury proceedings); Bivens v. Six Unknown Named Agents, 403 U.S. 388, 412-24 (1971) (Burger, C.J., dissenting) (questioning the wisdom of continued adherence to the exclusionary rule).

55. Boyd v. United States, 116 U.S. 616, 630 (1886).

56. Olmstead v. United States, 277 U.S. 438 (1928). In *Olmstead* the use of a wiretap to overhear the defendant's phone conversations was held not to constitute a search because there was no physical entry into a protected area and because the protection of the Fourth Amendment did not extend to intangibles such as conversation. *Id.* at 464-65. *See* Goldman v. United States, 316 U.S. 129 (1942) (no search where listening device was placed against defendant's hotel room wall).

57. Silverman v. United States, 365 U.S. 505 (1961). In *Silverman* a "spike mike" penetrated into the suspect's premises and contacted a heating duct, allowing the officers to hear conversations throughout the house. *Id.* at 506-07.

protection.[58] The illogic of continued adherence to the trespass doctrine was obvious, since the privacy interest invaded by electronic eavesdropping on conversations is the same whether or not a trespass has been committed.[59]

Meanwhile, a similar development was occurring with regard to visual observations by law enforcement officers. Following the maxim that the eye cannot commit a search,[60] the Court originally held that observation of activity in the "open fields" with the unaided eye is not within the protection of the Fourth Amendment.[61] This led to the development of the "plain view" doctrine: whenever a law enforcement officer is in a position where he has a right to be, and sees instrumentalities or fruits of crime, contraband or "mere evidence"[62] in plain view, it is not a violation of the Fourth Amendment for him to seize such items.[63] The doctrine applies even when officers use visual aids to extend the normal capability of the human eye. Thus the use of a flashlight at night to see what would have been visible to the naked eye during the day has been held not to constitute a search.[64] Similarly, observations made by the use of binoculars do not constitute a Fourth Amendment search.[65] When the officers made their observations during an unauthorized trespass onto the curtilage of an individual's property, however, a Fourth Amendment violation was found even though

58. Wong Sun v. United States, 371 U.S. 471, 485 (1963).

59. "[T]he invasion of privacy is as great in one case as in the other." Silverman v. United States, 365 U.S. 505, 512-13 (1961) (Douglas, J., concurring).

60. *See* McDonald v. United States, 335 U.S. 451, 454 (1948).

61. Hester v. United States, 265 U.S. 57 (1924).

62. *See* Warden v. Hayden, 387 U.S. 294 (1967).

63. Coolidge v. New Hampshire, 403 U.S. 443, 464-73 (1971) (plurality opinion); Harris v. United States, 390 U.S. 234 (1968). *See, e.g.*, Ker v. California, 374 U.S. 23, 43 (1963). In *Coolidge* it is stated that the viewing must be "inadvertent," but as this was the opinion of only a plurality of the Court, other courts, depending on the circumstances of the case, have sometimes held that "inadvertence" is not required. *E.g.*, State v. Pontier, 95 Idaho 707, 518 P.2d 969 (1974). *See, e.g.*, Weaver v. Williams, 509 F.2d 884 (4th Cir. 1975) (officer stepped onto axle of truck in order to see over siding): " 'Plain view' in this context means whatever can be seen, whether accidentally or by intentional scrutiny." *Id.* at 886. *See generally* Mascolo, *The Role of Functional Observation in the Law of Search and Seizure: A Study in Misconception*, 71 DICK. L. REV. 379 (1967).

64. *E.g.*, United States v. Lee, 274 U.S. 559 (1927); United States v. Booker, 461 F.2d 990 (6th Cir. 1972). *Contra*, Pruitt v. State, 389 S.W.2d 475 (Tex. Crim. App. 1965).

65. *E.g.*, United States v. Grimes, 426 F.2d 706 (5th Cir. 1970); Fullbright v. United States, 392 F.2d 432 (10th Cir.), *cert. denied*, 393 U.S. 830 (1968); *cf.* On Lee v. United States, 343 U.S. 747, 754 (1952) (dictum). *But see* People v. Ciochon, 23 Ill. App. 3d 363, 319 N.E.2d 332 (1974) (remanded on question of whether a reasonable expectation of privacy from binocular observation was exhibited).

no tangible objects were seized.[66] Again, with respect to visual observations the illogic of the trespass doctrine is apparent. The same privacy interest is invaded whether the observation is made during a trespass or by extrasensory means without the necessity of a trespass.

B. A "Reasonable Expectation of Privacy"

In *Berger v. New York*[67] the Court explicitly held that the use of electronic devices to capture conversation is a search within the meaning of the Fourth Amendment, without making reference to any trespass on the part of the electronic device into a "constitutionally protected area."[68] Shortly thereafter, in *Katz v. United States*,[69] the Court repudiated the trespass doctrine and returned to a focus on privacy as the primary determinant of whether a Fourth Amendment search and seizure had occurred.

In *Katz* the bugging of a telephone booth in order to overhear the suspect's side of phone conversations was held a violation of the Fourth Amendment in the absence of prior judicial authorization even though the listening device did not trespass into the phone booth. Holding that the Fourth Amendment "protects people, not places,"[70] and extends to "the recording of oral statements" as well as to "the seizure of tangible items,"[71] the Court concluded that "the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[72] By entering the phone booth and closing the door, the defendant exhibited a "reasonable expectation of privacy"[73] in his conversations. The bugging constituted a search and seizure under the Fourth Amendment because it "violated the privacy upon which [Katz] justifiably relied while using the telephone booth. . . ."[74]

The present test for determining when official conduct constitutes a

66. *E.g.*, California v. Hurst, 325 F.2d 891, 898 (9th Cir. 1963); McGinnis v. United States, 227 F.2d 598, 603 (1st Cir. 1955); Brock v. United States, 223 F.2d 681, 685 (5th Cir. 1955); *see* Wong Sun v. United States, 371 U.S. 471, 485 (1963) (dictum); McDonald v. United States, 335 U.S. 451, 453 (1948). The plain view doctrine is not applicable in such cases because the officer is not positioned where he has a right to be. *See* Coolidge v. New Hampshire, 403 U.S. 443, 465-66 (1971) (plurality opinion).

67. 388 U.S. 41 (1967).

68. *Id.* at 51.

69. 389 U.S. 347 (1967).

70. *Id.* at 351.

71. *Id.* at 353.

72. *Id.*

73. *Id.* at 360 (Harlan, J., concurring).

74. *Id.* at 353.

search or seizure is most clearly stated in Justice Harlan's concurrence in *Katz*:

> My understanding of the rule . . . is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[75]

C. Application to Electronic Snooping

The *Katz* decision does not affect the "plain view" doctrine because no one can have a reasonable expectation of privacy in an activity which can be viewed by the unaided senses of others.[76] But when a person

75. *Id.* at 361 (Harlan, J., concurring). A possible interpretation of this language is that whenever an actual expectation of privacy is absent, there is no Fourth Amendment search. One commentator has observed that if this interpretation is taken literally, "the government could diminish each person's subjective expectation of privacy merely by announcing half-hourly on television that 1984 was being advanced by a decade and that we were all forthwith being placed under comprehensive electronic surveillance." Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974) [hereinafter cited as Amsterdam]. At least one court has suggested this very method of eliminating an actual expectation of privacy. State v. Bryant, 287 Minn. 205, 211, 177 N.W.2d 800, 804 (1970) (store could eliminate expectation of privacy in public toilet stall by posting signs warning users of possible surveillance). *See* Comment, 55 MINN. L. REV. 1255 (1971); *cf.* United States v. Bynum, 485 F.2d 490, 501 (2d Cir. 1973), *vacated on other grounds*, 417 U.S. 903 (1974) (expectation of privacy could be eliminated by suspect's awareness that his phone was tapped); People v. Superior Court (Stroud), 37 Cal. App. 3d 836, 839, 112 Cal. Rptr. 764, 765 (1974) (no expectation of privacy from helicopter observation when the area was the subject of a regular air patrol). *But cf.* United States v. Davis, 482 F.2d 893, 905 (9th Cir. 1973) (expectation of privacy in airline carry-on luggage not diminished by frequency of intrusions). "Fortunately, neither *Katz* nor the fourth amendment asks what we expect of government. They tell us what we should demand of government." Amsterdam, *supra*, at 384. This note will assume that an actual expectation of privacy from electronic snooping could not be defeated in the manner suggested by a literal reading of Justice Harlan's phraseology.

76. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). A number of courts have held, in effect, that no expectation of privacy existed if there was *any* way in which a skillful and determined snooper could intrude using only his unaided senses. The burden is placed on the victim of the intrusion to guard his privacy against any conceivable invasion lest he lose it. *E.g.*, United States v. Vilhotti, 323 F. Supp. 425, 431 (S.D.N.Y. 1971); People v. Becker, 533 P.2d 494, 496 (Colo. 1975); Commonwealth v. Hernley, 216 Pa. Super. 177, 181, 263 A.2d 904, 907 (1970), *cert. denied*, 401 U.S. 914 (1971). This approach has produced vigorous criticism in light of the growing

takes reasonable steps to insure the actual privacy of his activity against visual intrusion, an invasion of that privacy which can only be accomplished by electronic means must be considered a search under the Fourth Amendment. Under the pre-*Katz* trespass doctrine, observations as well as conversations which were "seized" by means of an unlawful trespass were suppressed as having been obtained in violation of the Fourth Amendment.[77] The development of highly sophisticated electronic listening devices prompted the Court to declare that their use to capture conversation was a search regardless of whether a trespass had occurred.[78] Even in the absence of the *Katz* decision, the development of equally sophisticated electronic viewing devices would logically have led to the same result when observations were accomplished by the use of such devices.

Although *Katz* involved the specific problem of electronic eavesdropping, its explanation of a reasonable expectation of privacy was not so limited:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[79]

Furthermore, Justice Harlan's statement that activities exposed to plain view are excluded from Fourth Amendment protection[80] implies that activities not so exposed would be protected from observation.

Numerous other authorities recognize that the Fourth Amendment

---

sophistication of the means of intrustion. "Is it not important to our American way of life that when a citizen does as much as ordinary care requires to shield his sanctuary from strangers his constitutional right to maintain his privacy should not be made to depend upon the resources of skillful peepers and eavesdroppers who can always find ways to intrude?" United States v. Wright, 449 F.2d 1355, 1369 (D.C. Cir. 1971) (Wright, J., dissenting), *cert. denied*, 405 U.S. 947 (1972). After an extensive analysis of the cases dealing with plain view observations, one writer concludes that the result is "the specter of a fourth amendment which protects any man . . . who is wealthy enough to afford a windowless, soundproof house, built on an extensive area of land, and surrounded by high fences, and . . . who is willing to live the life of a hermit, staying inside his house at all times, prepared to take affirmative action to counter any new technological methods of intrusion with which the government might be equipped." Note, *Katz and the Fourth Amendment: A Reasonable Expectation of Privacy or, A Man's Home Is His Fort*, 23 CLEVE. ST. L. REV. 63, 72 (1974). *See* Amsterdam, *supra* note 75, at 402; Comment, *Police Helicopter Surveillance*, 15 ARIZ. L. REV. 145, 167 (1973); Comment, *Constitutional Standards for Applying the Plain View Doctrine*, 6 ST. MARY'S L.J. 725, 736, 741 (1974).

77. See notes 57-58, 66 *supra* and text accompanying.

78. See text accompanying note 68 *supra*.

79. Katz v. United States, 389 U.S. 347, 351-52 (1967) (citations omitted).

80. *Id.* at 361 (Harlan, J., concurring).

may protect an individual's activities from unwanted observation by electronic devices.[81] Absent prior judicial authorization, a camera lens which can view an area otherwise inaccessible to observation is not positioned where it has a right to be so that the plain view doctrine might apply.[82] The conclusion is inescapable: electronic snooping must be considered a search subject to the limitations imposed by the Fourth Amendment when it intrudes into an area where a reasonable expectation of privacy from observation exists. The next question to be considered, therefore, is whether electronic snooping can meet the standard of reasonableness prescribed by the Fourth Amendment.

IV. The Warrant Requirement and Electronic Snooping

A. Reasonableness and the Warrant Requirement

The judicial determination of Fourth Amendment reasonableness turns, "at least in part, on the more specific commands of the warrant clause."[83] In general, "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment . . . ."[84] It does not follow, however, that if a search has been authorized by a technically proper warrant it is automatically reasonable.[85] The Fourth Amendment's two clauses

81. "While the Katz case involved evidence obtained by listening and the case before us involves evidence obtained by visual observation, we think the results are the same." State v. Bryant, 287 Minn. 205, 210, 177 N.W.2d 800, 803 (1970). *See* People v. Spinelli, 35 N.Y.2d 77, 81n., 315 N.E.2d 792, 794n., 358 N.Y.S.2d 743, 747n. (1974) (recognition that a "technologically aided viewing" might in itself constitute a "constitutionally cognizable search"); Amsterdam, *supra* note 75, at 404; Knox, *Some Thoughts on the Scope of the Fourth Amendment and Standing to Challenge Searches and Seizures*, 40 Mo. L. Rev. 1, 17-18 (1975); Rehnquist, *Is an Expanded Right of Privacy Consistent With Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*, 23 U. Kans. L. Rev. 1, 4 (1974) (freedom from observation part of the "core" concept of privacy embodied in the Fourth Amendment).

82. See note 63 *supra* and text accompanying.

83. United States v. United States District Court, 407 U.S. 297, 315 (1972).

84. Katz v. United States, 389 U.S. 347, 357 (1967). *See* Camara v. Municipal Court, 387 U.S. 523, 528-29 (1967); Johnson v. United States, 333 U.S. 10, 14 (1948). Under certain conditions involving "exigent circumstances" making it unnecessary or unreasonable to obtain a warrant before conducting a search, prior judicial approval is unnecessary. The Court in *Katz* discounted the idea that any of these exceptions could apply to electronic eavesdropping. 389 U.S. at 357-58. The present discussion will make the same assumption as to electronic snooping. *But see* 18 U.S.C. § 2518(7) (1970), permitting electronic eavesdropping subject to subsequent judicial ratification within 48 hours in cases of emergency situations involving conspiratorial activities threatening national security or characteristic of organized crime.

85. Osborn v. United States, 385 U.S. 323, 350 (1966) (Douglas, J., dissenting), *citing* Boyd v. United States, 116 U.S. 616 (1886) ("a validly executed warrant does not

are to a certain extent independent. The first prohibits all unreasonable searches and seizures, and the second states the elements required for a valid warrant.[86] The present inquiry will consider these two clauses separately. The warrant requirement will first be discussed by analogy to the requirements for electronic eavesdropping orders. The general standard of reasonableness will then be applied to a judicial order for electronic snooping.

B. Constitutional Standards for Electronic Eavesdropping: Berger and Katz

In *Berger v. New York*[87] the Court considered the constitutionality of a New York statute which permitted electronic eavesdropping by law enforcement officers under specified conditions. The statute authorized a judge to issue an eavesdropping order upon oath or affirmation of an appropriate official stating the existence of reasonable ground to believe that evidence of crime would be obtained thereby, and particularly describing the persons whose conversations were to be overheard and the telephone number involved. The eavesdrop was limited to a two month period unless extended.[88]

Relying in part on the circumstances surrounding the judicially authorized use of an electronic recording device approved in *Osborn v. United States*,[89] the Court in *Berger* held the New York statute unconstitutional for the following reasons:

---

necessarily make legal the ensuing search and seizure"). *See, e.g.*, Bowden v. State, 510 S.W.2d 879 (Ark. 1974) (judicial order for surgery to remove bullet invalidated as authorizing an unreasonable search and seizure); *cf.* People v. Bracamonte, 15 Cal. 3d 394, 400 n.3, 540 P.2d 624, 628 n.3, 124 Cal. Rptr. 528, 532 n.3 (1975) (suggestion that certain bodily intrusions may not be constitutional even if authorized by search warrant). "Far from looking at the warrant as a protection against unreasonable searches, [our constitutional fathers] saw it as an authority for unreasonable and oppressive searches . . . ." T. TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 41 (1967).

86. "The Court has frequently observed that the Fourth Amendment's two clauses impose separate, although related, limitations upon searches and seizures; the first 'is general and forbids every search that is unreasonable'; the second places a number of specific constraints upon the issuance and character of warrants." Berger v. New York, 388 U.S. 41, 94 (1967) (Harlan, J., dissenting) (citation omitted). *See, e.g.*, Go-Bart Importing Co. v. United States, 282 U.S. 344, 356-57 (1931).

87. 388 U.S. 41 (1967).

88. *Id.* at 54.

89. 385 U.S. 323 (1966). In *Osborn* a recording device was concealed on the person of an informant pursuant to judicial authorization based on an affidavit detailing previous conversations between the informant and an attorney concerning the bribery of potential jurors in a pending criminal trial. *Id.* at 325-29.

1. Failure to require probable cause to believe that a "particular offense" has been or is being committed;[90]
2. Failure to require that the conversations sought be "particularly described";[91]
3. Authorization of "the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause" because of the sixty-day period of permissible surveillance, lack of a requirement of prompt execution, and lack of a requirement for present probable cause for an extension of the authorization;[92]
4. Failure to require termination of the eavesdrop once the conversation sought was obtained;[93]
5. Failure to require "some showing of special facts" to overcome the absence of notice necessarily resulting from the need for secrecy;[94] and

90. 388 U.S. at 58. "The purpose of the probable-cause requirement of the Fourth Amendment, to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed, is thereby wholly aborted." *Id.* at 59. In contrast, the affidavit in *Osborn* alleged "the commission of a specific criminal offense directly and immediately affecting the administration of justice . . . ." *Id.* at 57, *quoting* Osborn v. United States, 385 U.S. 323, 330 (1966).

91. *Id.* at 58-59. This failure "gives the officer a roving commission to 'seize' any and all conversations. . . . As with general warrants this leaves too much to the discretion of the officer executing the order." *Id.* at 59. In *Osborn* "the order described the *type of conversation* sought with particularity, thus indicating . . . the limitations placed upon the officer executing the warrant." *Id.* at 57 (emphasis added). "The need for particularity and evidence of reliability in the showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping. By its very nature eavesdropping involves an intrusion on privacy that is broad in scope." Thus " 'a heavier responsibility [is imposed] on this Court in its supervision of the fairness of procedures . . . .' " *Id.* at 56, *quoting* Osborn v. United States, 385 U.S. 323, 329 n.7 (1966).

92. *Id.* at 59. As a result "the conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation." *Id.* Authorization of an extension upon a showing that it would be "in the public interest" was held insufficient to constitute present probable cause. *Id.* In *Osborn* the order authorized only a single seizure of a conversation betweeen two known participants. A new order based on new probable cause was issued for a second seizure, and the orders were executed with dispatch. "In this manner no greater invasion of privacy was permitted than was necessary under the circumstances." *Id.* at 57.

93. *Id.* at 59-60. Termination was thus "left entirely in the discretion of the officer." *Id.* at 60. In *Osborn* "once the property sought, and for which the order was issued, was found the officer could not use the order as a passkey to further search." *Id.* at 57.

94. *Id.* at 60. "Such a showing of exigency, in order to avoid notice, would appear more important in eavesdropping, with its inherent dangers, than that required when

6. Failure to provide for a return on the warrant.[95]

The Court further clarified the constitutional standards for a valid electronic eavesdropping order in *Katz v. United States*.[96] In that case, government agents began their eavesdropping only after investigation had established strong probability that the telephone was being used in violation of federal law.[97] Surveillance was limited to the discovery of the contents of the communications, confined solely to the periods when the suspect was actually using the telephone booth, and conducted so that only the conversations of the suspect himself were overheard. The Court concluded that a magistrate "could constitutionally have authorized, with appropriate safeguards, the very limited search and seizure that the Government asserts in fact took place."[98] But even though the agents "reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end,"[99] the search was held unreasonable for failure to satisfy the constitutional precondition of prior judicial authorization.[100]

C. Title III Provisions

Relying on the guidelines provided by the Court in *Berger* and *Katz*, and spurred by rising crimes rates and calls for "law and order,"[101] Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[102] Title III prohibits the use of electronic eavesdropping to intercept wire or oral communications[103] without the con-

conventional procedures of search and seizure are utilized." *Id.* The Court made no specific reference, however, to any such showing in *Osborn*.

95. *Id.* The statute thereby left "full discretion in the officer as to the use of seized conversations of innocent as well as guilty parties." *Id.* In *Osborn* "the officer was required to and did make a return on the order showing how it was executed and what was seized." *Id.* at 57.

96. 389 U.S. 347 (1967). See text accompanying notes 69-75 *supra*.

97. *Id.* at 354.

98. *Id.*

99. *Id.* at 356-57.

100. *Id.* at 359.

101. *See* Schwartz, *The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order,"* 67 MICH. L. REV. 455-56 (1969).

102. 18 U.S.C. §§ 2510-2520 (1970).

103. *Id.* § 2511(1) (1970). "Wire communications" are communications made over telephone or telegraph lines. *Id.* § 2510(1) (1970). "Oral communications" are "any oral communication[s] uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." *Id.* § 2510(2) (1970). "Intercept" is defined as "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4) (1970).

sent of one of the parties to the communication[104] except under carefully limited conditions for law enforcement purposes. The strict procedural requirements of Title III, derived from the constitutional standards prescribed by *Berger* and *Katz*, are contained in section 2518.[105]

First, this section requires that an application for an interception order be supported by "a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued."[106] A judge may issue an order only upon a finding of treble probable cause, that is, probable cause to believe that:

1. An individual has committed, is committing, or is about to commit a particular offense;[107]
2. Particular communications concerning that offense will be obtained through such interception;[108] and
3. The facilities from which, or the place where, the wire or oral communications are to be intercepted are being used,

104. Interception with the consent of one of the parties to the communication is not prohibited. *Id.* § 2511(2)(c) (1970). Such "consent" eavesdropping is not considered a search and seizure under the Fourth Amendment. United States v. White, 401 U.S. 745 (1971); Osborn v. United States, 385 U.S. 323 (1966); Lopez v. United States, 373 U.S. 427 (1963); On Lee v. United States, 343 U.S. 747 (1952). *Contra*, People v. Beavers, 393 Mich. 554, 227 N.W.2d 511 (1975), *cert. denied*, 96 S. Ct. 152 (1975) (relying on state constitution). The theory is that no one can have a reasonable expectation "that a person with whom he is conversing will not then or later reveal the conversation to the police." United States v. White, 401 U.S. 745, 749 (1971) (plurality opinion). For constitutional purposes the use of a tape recorder or transmitter to make the report to the police is irrelevant. 401 U.S. at 751 (plurality opinion).

An analogous problem could arise in the use of electronic snooping technology. For example, an informant could carry a briefcase containing a concealed camera, or indeed could have a minature camera lens concealed on his person. See text accompanying note 38 *supra*. Acts of the suspect with whom the informant was meeting could be transmitted to a remote location for videotaping. A mechanical application of the *White* rationale would lead to the conclusion that there was no reasonable expectation that the informant would not report to the police the suspect's appearance, physical description, and activities that he observed, and that a surreptitiously made videotape recording is merely a more accurate way to make such a report. A videotape recording, however, would convey considerably more information about a person than a recording of his spoken words. Such an intrusion should at least be considered a search under the Fourth Amendment. "Although one assumes the risk that a guest may verbally divulge his appearance he does not assume the risk that the same guest may photograph him without his consent." Comment, *Consent to Electronic Surveillance by a Party to a Conversation: A Different Approach*, 10 TULSA L.J. 386, 389 (1975).

105. 18 U.S.C. § 2518 (1970). *See* SENATE REPORT, *supra* note 7, at 88-108.

106. 18 U.S.C. § 2518(1)(b) (1970).

107. *Id.* § 2518(3)(a) (1970).

108. *Id.* § 2518(3)(b) (1970).

or are about to be used, in connection with the commission of such offense.[109]

Second, in satisfaction of the particularity requirement the statement of facts and circumstances must include:

1. Details as to the particular offense that has been, is being, or is about to be committed;
2. A particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted;
3. A particular description of the type of communication sought to be intercepted; and
4. The identity of the person, if known, committing the offense and whose communications are to be intercepted.[110]

Third, the applicant must make a statement of the period of time for which the interception is required to be maintained.[111] If additional communications of the same type are expected, the facts establishing probable cause to believe that such additional communications will occur after the first one has been obtained must be particularly described.[112] The order may authorize interception only for as long as necessary to achieve the objective of the authorization and in no event longer than thirty days.[113] In addition, every interception must be conducted in such a way as to minimize the interception of communications not otherwise subject to interception.[114]

Finally, the application must contain a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear unlikely to succeed if tried or to be too dangerous.[115] An order may be issued only if the judge finds, upon the facts presented by the applicant, that normal investigative procedures

109. *Id.* § 2518(3)(d) (1970).

110. *Id.* § 2518(1)(b) (1970). *See* United States v. Kahn, 415 U.S. 143 (1974).

111. 18 U.S.C. § 2518(1)(d) (1970).

112. *Id.*

113. *Id.* § 2518(5) (1970). Extensions for up to 30 days may be obtained upon a new showing of probable cause. *Id.*

114. *Id. See generally* Note, *Minimization and the Fourth Amendment*, 19 N.Y.L.F. 861 (1974) (constitutional basis of the minimization requirement); Note, *Minimization of Wire Interception: Presearch Guidelines and Postsearch Remedies*, 26 STAN. L. REV. 1411 (1974).

115. 18 U.S.C. § 2518(1)(c) (1970). *See generally* Note, *Electronic Surveillance, Title III, and the Requirement of Necessity*, 2 HAST. CONST. L.Q. 571 (1975).

have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.[116]

D. Procedural Requirements for an Electronic Snooping Order

Central to the Court's decision in *Berger* was its recognition that without a carefully circumscribed authorization procedure the use of electronic eavesdropping would constitute a general search in violation of the Fourth Amendment.[117] In order to avoid this result the Court emphasized throughout its opinion the need to eliminate any discretion on the part of the officer executing the order.[118] The Court summarized its holding by finding that the New York statute in question was "without adequate judicial supervision or protective procedures."[119]

Title III has been found constitutional on the ground that its provisions are "as precise and discriminate . . . as are the demands of *Berger* and *Katz*."[120] To the extent that Title III's provisions tend to restrict the executing officers' discretion, therefore, they may be said to be constitutionally based on *Berger*'s demand for adequate protective procedures. Moreover, to the extent that any clandestine electronic intrusion upon an individual's privacy would constitute a general search in the absence of such protective procedures, *Berger* and Title III may be said to indicate a broad outline of the facial requirements of any electronic surveillance order. The next section will discuss the reasonableness of electronic snooping with respect to four requirements that appear to be constitutionally mandated: particularity, length of surveillance, minimization and necessity.

V. Is Electronic Snooping Reasonable?

The oft-repeated rule for determining the reasonableness of a Fourth Amendment search is that a balancing test is to be utilized: "[T]here can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails."[121]

In practice electronic snooping might be used in conjunction with a

116. 18 U.S.C. § 2518(3)(c) (1970).

117. 388 U.S. at 58.

118. *Id.* at 57-60. See notes 91, 93, 95 *supra.*

119. *Id.* at 60.

120. United States v. Cafero, 473 F.2d 489, 495 (3d Cir. 1973), *cert. denied*, 417 U.S. 918 (1974), *quoting* United States v. Cox, 449 F.2d 679, 687 (10th Cir. 1971), *cert. denied*, 406 U.S. 934 (1972).

121. Camara v. Municipal Court, 387 U.S. 523, 536-37 (1967).

listening device authorized under Title III, thus providing an accurate visual record of the events which took place during a valid electronic eavesdrop.[122] This does not imply, however, that the constitutional standards governing the use of the listening device similarly would authorize the use of the camera. Because of the significantly different privacy interests invaded by its use, the reasonableness of electronic snooping must be evaluated on its own terms by reference to the balancing test. This evaluation requires an examination of the law enforcement justification for electronic snooping and the extent to which it intrudes upon personal privacy. In considering the constitutionality of this latest method for clandestine intrusion upon individual privacy, it is important to keep in mind a twice-repeated warning of the Supreme Court:

> It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure.[123]

A. Procedural Requirements in Factual Context

1. Particularity

Electronic snooping could be utilized either to view a "private act,"[124] in a manner similar to electronic eavesdropping on private conversations, or to observe a particular tangible object[125] and to record its presence in the area under surveillance. In either case the first consideration is the degree of particularity required of the application and order.

The issuance of an electronic snooping order would require the existence of probable cause to believe that a specific offense[126] was under investigation and that at an identifiable location[127] particular acts or objects related to the commission of that offense would be ob-

122. For example, see text accompanying note 1 *supra*.

123. Silverman v. United States, 365 U.S. 505, 512 (1961), *quoting* Boyd v. United States, 116 U.S. 616, 635 (1886).

124. A "private act" may be defined, by analogy to electronic eavesdropping, as an act performed by a person exhibiting an expectation that such act is not subject to viewing under circumstances justifying such expectation. See note 103 *supra*.

125. Electronic snooping might be employed for this purpose when the object is one which may be easily disposed of or destroyed. By recording the object's presence in the area under surveillance, its evidentiary value would be preserved even if it were not seized intact in a subsequent physical search. For example, such objects might include narcotics paraphernalia or gambling records.

126. See notes 90, 107 *supra* and text accompanying.

127. See text accompanying note 110 *supra*.

79-064 O - 76 - 79

served.[128] Presumably a detailed description of the "type of act"[129] or of the specific tangible object[130] would sufficiently describe the thing to be seized. An adequate description of the place to be searched would be more difficult. A camera's usefulness is necessarily limited to observation of acts or objects within the room where the camera is located. Therefore, the application and order would have to specify the precise location *within* the premises where the acts were expected to take place or the objects were expected to be located.[131] This particularity is necessary for the existence of probable cause to believe that the officer's placement of the camera will actually reveal the acts or objects to be viewed.[132] In the absence of such an exacting requirement the officer could exercise his own discretion as to the placement of the camera, thereby permitting the search of unauthorized areas in violation of the requirements of *Berger*.[133]

2. Length of Surveillance

An electronic snooping order could presumably authorize observation of private acts over a period of time sufficient to attain the objective

128. See text accompanying note 108 *supra*. This would indicate "the specific objective of the Government . . . and the limitations placed upon the officer executing the warrant." Berger v. New York, 388 U.S. 41, 57 (1967).

129. See note 91 *supra* and text accompanying. An act, like an oral communication, cannot be more particularly described until after it has occurred. *See* United States v. Tortorello, 480 F.2d 764, 780 (2d Cir.), *cert. denied*, 414 U.S. 866 (1973).

130. *See* Marron v. United States, 275 U.S. 192, 196 (1927). *See generally* Cook, *Requisite Particularity in Search Warrant Authorizations*, 38 TENN. L. REV. 496, 505-07 (1971).

131. For example, the criminal acts might be taking place in a bedroom; installation of a camera in the living room would be useless.

132. This problem clearly does not exist when wiretapping is employed; identification of the premises where the telephone to be tapped is located provides sufficient particularity as to the place to be searched. The absence of a similar problem with respect to "bugging" is not so clear, at least when conversations in a multiroom house or similar premises are to be overheard. Due to the relatively small number of bugging authorizations, the precise problem may not have arisen. See note 153 *infra*. Also, bugging frequently may be conducted under circumstances permitting the interception of all conversations because of the limited size of the premises under surveillance. *See* Katz v. United States, 389 U.S. 347 (1967) (phone booth); Berger v. New York, 388 U.S. 41 (1967) (law office); Goldman v. United States, 316 U.S. 129 (1942) (hotel room). Finally, the eavesdropping method employed may enable the overhearing of conversations throughout the entire premises. *See* Silverman v. United States, 365 U.S. 505 (1961) ("spike mike" contacting heating duct).

133. 388 U.S. at 57. As an alternative, cameras might be installed in *each* room on the premises where it is likely that the acts or objects will be viewed. However, this procedure might well constitute such a "broadside authorization" as to result in "general searches by electronic devices" of the type condemned in *Berger*. *Id.* at 58. *See id.* at 65 (Douglas, J., concurring); *cf.* Irvine v. California, 347 U.S. 128 (1954).

of the snooping. Termination upon observation of an incriminating act would not be required if probable cause existed to believe that similar acts would thereafter occur.[134] A different situation would exist, however, if the order authorized a search for a tangible object. In order to satisfy the particularity requirement as to the place to be searched, there would have to be probable cause to believe that the object would be viewed in the particular room where the camera was installed, at the time the camera was activated.[135] If the object were not observed at that time, the probable cause to believe that it would be observed would no longer exist. Without a new authorization based on new probable cause, a subsequent search for the same object would be invalid as constituting "a series of intrusions, searches, and seizures pursuant to a single showing of probable cause."[136]

The result is that electronic snooping for a tangible object could only be used on a "one-time-only" basis. For each showing of probable cause, the camera could be activated only once and left on only as long as reasonably necessary to determine the presence or absence of the item in question. If the item were observed, the objective of the authorization would be accomplished and the observation would have to be terminated.[137] If it were not observed, the officers could not unreasonably prolong their search or expand it with the hope of seeing something incriminating beyond the scope of their authorization.[138]

3. Minimization

Title III requires that every interception of wire or oral communications be conducted in such a way as to minimize the interception of communications not otherwise subject to interception.[139] While the specific form of this provision has been referred to as a "statutory command,"[140] the principle which it embodies is clearly constitutionally based. The Court has held that "a search which is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable

134. See text accompanying notes 111-113 *supra*. Title III's limitation of 30 days is a maximum, and can be shortened by the authorizing judge on a case-by-case basis depending on the specific objective of the interception. *See* United States v. Cafero, 473 F.2d 489, 495 (3d Cir. 1973), *cert. denied*, 417 U.S. 918 (1974).

135. See text accompanying note 131 *supra*.

136. Berger v. New York, 388 U.S. 41, 59 (1967). *See* Sgro v. United States, 287 U.S. 206, 211 (1932).

137. Berger v. New York, 388 U.S. 41, 57 (1967).

138. *Id.*

139. 18 U.S.C. § 2518(5) (1970). See text accompanying note 114 *supra*.

140. *E.g.*, United States v. Cox, 462 F.2d 1293, 1300 (8th Cir. 1972), *cert. denied*, 417 U.S. 918 (1974).

intensity and scope."[141] Lack of an attempt to minimize interception of innocent or irrelevant conversations results in the seizure of "the conversations of any and all persons coming into the area covered by the device . . . without regard to their connection with the crime under investigation."[142] Electronic eavesdropping conducted in this manner, even pursuant to a properly particularized court order, would undoubtedly be of such "intolerable intensity and scope" as to be unreasonable.[143] Moreover, minimization has been referred to as one of the "protective procedures"[144] by which the electronic eavesdropping authorized by Title III is found to be reasonable.[145] Thus Title III's minimization requirement appears to be based upon the constitutional limitations inherent in any Fourth Amendment search as well as upon *Berger's* procedural safeguards against the inherent dangers of clandestine surveillance. By analogy, it will be assumed that minimization in the execution of an electronic snooping order similarly would be constitutionally mandated.

Compliance with the minimization requirement is to be measured by whether "on the whole the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion."[146] Minimization is accomplished by avoiding interception of all calls falling within nonpertinent categories, as soon as

141. Terry v. Ohio, 392 U.S. 1, 18 (1968); *see* Von Cleef v. New Jersey, 395 U.S. 814 (1969); Kremen v. United States, 353 U.S. 346 (1957); People v. Bracamonte, 15 Cal. 3d 394, 400, 540 P.2d 624, 628, 124 Cal. Rptr. 528, 532 (1975).

142. Berger v. New York, 388 U.S. 41, 59 (1967).

143. *See* United States v. United States District Court, 407 U.S. 297, 326 (1972) (Douglas, J., concurring); Von Cleef v. New Jersey, 395 U.S. 814, 817 (1969) (Harlan, J., concurring in the result); United States v. George, 465 F.2d 772 (6th Cir. 1972). *See generally* Note, *Minimization and the Fourth Amendment*, 19 N.Y.L.F. 861, 875-78 (1974).

144. Berger v. New York, 388 U.S. 41, 60 (1967). See text accompanying notes 117-120 *supra.*

145. United States v. Kahn, 415 U.S. 143, 154 (1974); United States v. Focarile, 340 F. Supp. 1033, 1038, 1044 (D. Md.), *aff'd on other grounds sub nom.* United States v. Giordano, 469 F.2d 522 (4th Cir. 1972), *aff'd*, 416 U.S. 505 (1974); United States v. King, 335 F. Supp. 523, 532, 541 (S.D. Cal. 1971), *modified on other grounds*, 478 F.2d 494 (9th Cir. 1973), *cert. denied*, 417 U.S. 920 (1974); United States v. Leta, 332 F. Supp. 1357, 1360 (M.D. Pa. 1971); *see* Bynum v. United States, 96 S. Ct. 357 (1975) (Brennan, J., dissenting from denial of certiorari).

146. United States v. Tortorello, 480 F.2d 764, 784 (2d Cir.), *cert. denied*, 414 U.S. 866 (1973); *see* United States v. Scott, 504 F.2d 194, 198-99 (D.C. Cir. 1974). Factors to be taken into account in determining the reasonableness of minimization procedures include the scope of the criminal enterprise under investigation, the location and operation of the subject telephone, whether a pattern of incriminating conversations emerges, and the degree of supervision by the authorizing judge. United States v. James, 494 F.2d 1007, 1019-21 (D.C. Cir.), *cert. denied*, 419 U.S. 1020 (1974).

the agents have sufficient information to establish such categories.[147] These principles allow the minimization procedures applicable to electronic snooping to be compared and contrasted with those used in wiretapping and bugging.

a. Analogy to Wiretapping

The officers executing a wiretap order normally become aware of the commencement of a conversation whose interception may be authorized by the occurrence of a trigger "signal" in the form of either the ringing or the dialing of the tapped telephone. A minimization decision based on the contents of the communication can be made within a short time thereafter.[148] Thus the privacy of the premises where the phone is located is invaded by a wiretap only when an activity of the type whose seizure has been authorized is actually in progress. The minimization requirement insures that the invasion of privacy will terminate promptly if the conversation is not in an incriminating category. In addition, a wiretap only invades the privacy of the actual parties to the conversation. In this way the objective of the authorization is fulfilled while "the danger of an unlawful search and seizure [is] minimized."[149]

An attempt to fulfill the objective of an electronic snooping order, however, necessarily involves a much more indiscriminate intrusion. Although probable cause would exist to believe that incriminating acts would be viewed on the premises, there would be no signal, as in the case of wiretapping, to alert the snoopers to the commencement of an act whose viewing might be authorized. The snoopers would presumably have to "tune-in" on the premises at random intervals in order to determine whether an act was occurring which might properly be observed. Such intrusions might view only an empty room or an individual engaged in no activity, so that the minimization requirement would dictate that the intrusion terminate. Shortly after the termination,

147. United States v. Scott, 516 F.2d 751, 754-55 (D.C. Cir. 1975); United States v. Tortorello, 480 F.2d 764, 785 (2d Cir.), *cert. denied*, 414 U.S. 866 (1973). But interception of calls of short duration need not be terminated before the nature of the calls and the identities of the parties can be determined. United States v. Bynum, 485 F.2d 490, 500 (2d Cir. 1973), *vacated on other grounds*, 417 U.S. 903 (1974).

148. This is subject to the qualification that conspirators who know they may be under surveillance frequently use code words or deliberately discuss innocent matters at the beginning of a call, which may justify a longer period of listening to determine the actual nature of the call. *See* United States v. Armocida, 515 F.2d 29, 39 n.12 (3d Cir. 1975); United States v. Quintana, 508 F.2d 867, 874-75 n.6 (7th Cir. 1975); United States v. James, 494 F.2d 1007, 1019 (D.C. Cir.), *cert. denied*, 419 U.S. 1020 (1974).

149. Berger v. New York, 388 U.S. 41, 57 (1967).

however, acts might take place whose viewing in fact was authorized. Without a signal to alert them that such an act was occurring the snoopers would be unaware of it and the objective of the authorization would be frustrated.

From a practical standpoint, therefore, the effectiveness of electronic snooping in attaining its objective might be seriously undermined unless the snooping were virtually continuous. Only in this way would the agents, not knowing when an incriminating act was likely to occur, have a reasonable chance of actually observing the act when it did occur. While this might be all that the agents reasonably could do to avoid unnecessary intrusion and still accomplish their objective, the resulting invasion of privacy might well exceed the "precise and discriminate" standard required by *Berger*[150] and *Katz*.[151]

b. Analogy to Bugging

No cases have been found which deal with the question of minimization in the context of electronic bugging. Presumably the minimization requirement applies to the extent that it is consistent with the effectiveness of the bug.[152] In such cases a "tune-in" procedure such as described above for electronic snooping would seem to be appropriate.[153] To this extent the two surveillance techniques would be on an

150. *Id.*

151. 389 U.S. at 355.

152. Situations are conceivable in which the continuous monitoring of a listening device for a limited period of time might be fully justified, such as for surveillance of a meeting of organized crime leaders or other known conspirators. Some courts have upheld the continuous monitoring of all telephone conversations as a reasonable compliance with the minimization requirement when virtually all conversations were incriminating or when no predictable pattern or category of innocent calls could be determined. United States v. Scott, 516 F.2d 751, 758-60 (D.C. Cir. 1975); United States v. Quintana, 508 F.2d 867, 873 (7th Cir. 1975); United States v. James, 494 F.2d 1007, 1018-23 (D.C. Cir.), *cert. denied*, 419 U.S. 1020 (1974); United States v. Manfredi, 488 F.2d 588, 600 (2d Cir. 1973), *cert. denied*, 417 U.S. 936 (1974); United States v. Bynum, 485 F.2d 490, 500 (2d Cir. 1973), *vacated on other grounds*, 417 U.S. 903 (1974); United States v. Cox, 462 F.2d 1293, 1301 (8th Cir. 1972), *cert. denied*, 417 U.S. 918 (1974). With respect to minimization, the continuous use of electronic snooping in such situations would presumably be valid as well.

153. As in the case of electronic snooping, however, it might be difficult to properly minimize interception of innocent conversations in this way and still intercept the information for which the eavesdrop was authorized. This difficulty may be a significant factor in the very low percentage of Title III authorizations for bugging rather than wiretapping. *See, e.g.*, ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS FOR THE PERIOD JANUARY 1, 1973 TO DECEMBER 31, 1973, at 16 (1974) [hereinafter cited as 1973 REPORT] (90% of all authorizations were for phone wire interceptions).

equal footing with respect to the reasonableness of their minimization procedures.[154]

Aside from the greater personal interest invaded by electronic snooping, however, even a valid attempt to minimize observation of innocent acts would entail a more severe intrusion upon privacy than minimization in the context of electronic eavesdropping. An electronic eavesdropping tune-in might result in overhearing nothing at all, if no conversations were taking place at the time of the intrusion. The visual tune-in, however, would always see something, even if only an empty room. In both cases a search has taken place, because of the intrusion into an area protected by a reasonable expectation of privacy.[155] But when nothing is overheard there has been no seizure of an individual's private conversations, whereas the visual observation constitutes a simultaneous search and seizure.[156] The visual tune-in "seizes" a view of an area protected by a reasonable expectation of privacy against such viewing even when no private acts are observed. Due to the nature of electronic snooping, therefore, even minimization procedures identical to those used in electronic eavesdropping will result in a more serious intrusion upon personal privacy.

4. Necessity

Title III provides that an interception order may be issued only if the judge finds that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.[157] That this provision supplies the "exigency" demanded by *Berger*[158] in order to avoid presearch notice to the victim of a clandestine intrusion is now generally recognized.[159] This requirement also follows directly from the Fourth Amendment balancing test: if "the scope of the particular intrusion, in light of all the exigencies of

154. Neither the Court nor Title III makes a constitutional distinction between wiretapping and bugging, despite the arguably greater breadth of the intrusion resulting from the use of listening devices. *See* United States v. Escandar, 319 F. Supp. 295, 301 (S.D. Fla. 1970), *remanded on other grounds sub nom.* United States v. Robinson, 472 F.2d 973 (5th Cir. 1973) (per curiam). Indeed, both *Berger* and *Katz* involved interception of communications by bugging rather than wiretapping.

155. Katz v. United States, 389 U.S. 347 (1967).

156. "The Government's activities in electronically *listening to* and *recording* the petitioner's words . . . constituted a 'search and seizure' within the meaning of the Fourth Amendment." *Id.* at 353 (emphasis added).

157. 18 U.S.C. § 2518(3)(c) (1970).

158. 388 U.S. at 60.

159. *See* Note, *Electronic Surveillance, Title III, and the Requirement of Necessity*, 2 HAST. CONST. L.Q. 571, 577-86 (1975), and cases cited therein at 585 n.77.

the case,"[160] exceeds what is reasonably necessary to accomplish a legitimate law enforcement goal, the intrusion should be declared unreasonable.[161]

The reasonableness of electronic snooping will therefore depend on whether other less intrusive techniques can be utilized to accomplish the same law enforcement objective. Now, however, these currently available less intrusive techniques include electronic eavesdropping. Whenever the same objective can be accomplished by a conventional search and seizure, or by a conventional search and seizure supplemented with electronic eavesdropping, electronic snooping will fail to satisfy the necessity requirement.

B. Application of the Necessity Requirement

1. Viewing of Tangible Objects

As discussed above,[162] electronic snooping for tangible objects where destruction of the evidence is feared would be limited to use on a one-time-only basis, for if the authorized observation did not reveal the object the probable cause supporting the order would no longer exist. This one-time-only use of electronic snooping, however, should be held unreasonable for failure to satisfy the necessity requirement.

In *Ker v. California*,[163] the Court recognized a judicial exception to the general requirement that the officers executing a search warrant announce their identity and purpose before entering in cases where they reasonably believe that the announcement will provoke the destruction of critical evidence.[164] This exception permits the accomplishment of

160. Terry v. Ohio, 392 U.S. 1, 18 n.15 (1968).

161. It may be that in the context of conventional searches and seizures, a search is not made unreasonable simply because the public interest could have been protected in a less intrusive manner. *See* Cady v. Dombrowski, 413 U.S. 433, 447 (1973). The *Berger* opinion made it clear, however, that in the case of electronic surveillance, a "heavier responsibility" is placed on the Court because of the broad scope and inherent dangers involved. 388 U.S. at 56. As interpreted by lower courts, *Berger* may in fact state a doctrine of "less intrusive means" when considering the reasonableness of any kind of clandestine electronic surveillance. "[T]he Court has long been critical of secret searches. Electronic surveillance cannot be justified unless other methods of investigation are not practicable." United States v. Tortorello, 480 F.2d 764, 774 (2d Cir.), *cert. denied*, 414 U.S. 866 (1973) (citation omitted). It is "a touchstone consideration in surveillance that 'no greater invasion of privacy [be] permitted than was necessary under the circumstances.'" United States v. Martyniuk, 395 F. Supp. 42, 44 (D. Or. 1975), *quoting* Berger v. New York, 388 U.S. 41, 57 (1967). *See* Comment, *Police Helicopter Surveillance*, 15 ARIZ. L. REV. 145, 170 (1973).

162. See text accompanying notes 135-38 *supra*.

163. 374 U.S. 23 (1963).

164. *Id.* at 37-41. *See* Katz v. United States, 389 U.S. 347, 355-56 n.16 (1967).

the same objective as electronic snooping with much less serious consequences to the individual's privacy.[165] Since the needs of law enforcement can be met[166] by use of this judicial exception to the notice requirement, the use of electronic snooping to determine the presence of tangible objects should be considered unreasonable under the Fourth Amendment.

2. Viewing of "Private Acts"

The need for the use of electronic eavesdropping in law enforcement stems primarily from its unique ability to acquire information in certain kinds of cases involving organized crime, gambling conspiracies or drug rings,[167] which is vital to the successful prosecution of these offenses and can be acquired in no other way.[168] Title III was intended specifically as a tool to combat organized crime, and is considered particularly useful for this purpose because of the dependence of organized crime on telephone communications to coordinate its worldwide

165. Justice Brennan objected to this judicial exception to the "announcement of purpose" requirement on the ground that "[i]nnocent citizens should not suffer the shock, fright or embarrassment attendant upon an unannounced police intrusion." Ker v. California, 374 U.S. 23, 57 (Brennan, J., dissenting). The Court in *Katz* discounted the idea that this objection would be relevant to electronic eavesdropping. 389 U.S. at 355-56 n.16. This should not be taken to indicate that electronic snooping would somehow have less serious consequences upon a person's privacy than an unannounced police intrusion. Shock fright and embarrassment would be felt as a result of an unannounced police intrusion whether the intrusion was direct and physical or indirect by means of an electronic eye. The latter invasion would in fact have more serious consequences for the individual's sense of security simply because an individual can adjust his conduct in an appropriate manner upon becoming aware of a physical intrusion, whereas he may not learn of the electronic invasion until long afterwards.

166. The officers would need probable cause to believe that the object would be found in a certain location within the premises before sufficient particularity for the issuance of an electronic snooping order would exist. See notes 131-33 *supra* and text accompanying. Similarly there would have to be probable cause to believe that the object would be observed in plain view, because otherwise television observation would be useless. With such a high degree of particularity an unannounced physical intrusion would almost certainly accomplish the seizure successfully, because the officers would know exactly where to look.

167. Narcotics and gambling cases comprise the great bulk of the investigations in which electronic eavesdropping is authorized. *See, e.g.*, 1973 REPORT, *supra* note 153, at 8 (75% of all intercept orders were for gambling or narcotics).

168. The factors rendering conventional investigative methods ineffective in organized crime investigations include the insulation of street workers known to police from the leaders of the conspiracies, a code of silence preventing testimony of those who might be able to provide evidence against the leaders, and the inability of informants to penetrate the conspiracy. *See generally* PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 198-201 (1967) [hereinafter cited as THE CHALLENGE OF CRIME IN A FREE SOCIETY].

activities.[169] However, because of its "inherent dangers,"[170] electronic eavesdropping cannot be considered reasonable except when other less intrusive methods of acquiring the same information prove inadequate.[171] Similarly, electronic snooping would be permissible only if it would provide information to law enforcement agencies which is both essential and currently unavailable through the use of conventional methods, including electronic eavesdropping.

In the investigation of gambling conspiracies, for example, the interception of telephone communications may be the only way to gather the critical information necessary for a successful prosecution. Large-scale gambling conspiracies conduct their operations almost exclusively by telephone, the members of the conspiracy generally keep meager written records, and informants are normally unable to gain access to the overall scheme.[172] Physical surveillance is normally ineffective because "there is little or no personal contact between these persons."[173] In the case of federal prosecutions, without wiretapping it may be impossible to establish "the interstate nature of the gambling operation."[174]

These arguments provide no justification for the additional use of electronic snooping in gambling investigations. If there is little or no personal contact between the members of a gambling conspiracy, a camera would provide little or no evidence of gambling transactions which cannot be acquired currently through electronic eavesdropping. The most that a strategically located camera might provide would be visual evidence of money changing hands, which would tend to corroborate the intercepted conversations concerning the illegal transactions but would not constitute independent evidence of a crime by itself or lead to conspirators who cannot be identified otherwise. It is unlikely

169. SENATE REPORT, *supra* note 7, at 70-71.

170. Berger v. New York, 388 U.S. 41, 60 (1967).

171. 18 U.S.C. § 2518(1)(c) & (3)(c) (1970). However, electronic eavesdropping is not necessarily barred by the necessity requirement even if an informant is available to testify or if probable cause for an arrest is present. *See* United States v. Staino, 358 F. Supp. 852, 857 (E.D. Pa. 1973); United States v. Lanza, 356 F. Supp. 27, 30 (M.D. Fla. 1973). Frequently the objective of the interception is to identify other members of a conspiracy who are as yet unknown to both the police and the informant. *See, e.g.*, United States v. Armocida, 515 F.2d 29, 38 (3d Cir. 1975); Note, *Electronic Surveillance, Title III, and the Requirement of Necessity*, 2 HAST. CONST. L.Q. 571, 613 n.176 (1975) (averment to this effect contained in every wiretap application examined).

172. *See, e.g.*, United States v. Bobo, 477 F.2d 974, 982-83 (4th Cir. 1973), *cert. denied*, 421 U.S. 909 (1975).

173. *Id.* at 983 (agent's affidavit).

174. *Id.*; *see, e.g.*, United States v. Leta, 332 F. Supp. 1357, 1362 (M.D. Pa. 1971).

that visual observation of a closed area would provide evidence of the interstate nature of the operation. In fact, interception of long distance phone calls appears to be an ideal method of acquiring such evidence.[175] Also, due to the absence of written records little tangible evidence would normally be observed by a hidden camera in gambling cases. Moreover, there is no indication at present that properly restricted electronic eavesdropping is ineffective in the investigation and prosecution of gambling conspiracies. Therefore there is no apparent law enforcement need for the additional tool of electronic snooping, because there is no showing that its use would result in the conviction of gamblers who presently escape prosecution.

Similarly, at present there is no indication of the necessity for electronic snooping in the investigation and prosecution of large narcotics operations. Electronic eavesdropping has proven to be an effective technique in cases involving the use of telephone facilities to coordinate the world-wide shipment and distribution of narcotics.[176] Conventional investigative techniques are often ineffective because of the inability of informants to penetrate the conspiracy and the drug dealer's extreme caution.[177]

If the leaders of a narcotics conspiracy use the telephone exclusively to direct the operation without face-to-face meetings with other members of their distributing network, interception of these telephone conversations would provide the evidence necessary to prove the crime and electronic snooping would serve no additional purpose.[178] Possibly

175. *See* United States v. Cafero, 473 F.2d 389, 493 (3d Cir. 1973), *cert. denied*, 417 U.S. 918 (1974).

176. *See* United States v. Focarile, 340 F. Supp. 1033, 1042-43 (D. Md.), *aff'd on other grounds sub nom.* United States v. Giordano, 469 F.2d 522 (4th Cir. 1972), *aff'd*, 416 U.S. 505 (1974); United States v. King, 335 F. Supp. 523, 535 (S.D. Cal. 1971), *modified on other grounds*, 478 F.2d 494 (9th Cir. 1973), *cert. denied*, 417 U.S. 920 (1974); United States v. Scott, 331 F. Supp. 233, 242 (D.D.C. 1971), *vacated on other grounds*, 504 F.2d 194 (D.C. Cir. 1974); United States v. Escandar, 319 F. Supp. 295, 303 (S.D. Fla. 1970), *remanded sub nom.* United States v. Robinson, 472 F.2d 973 (5th Cir. 1973) (per curiam).

177. *See, e.g.*, United States v. Armocida, 515 F.2d 29, 38 (3d Cir. 1975); United States v. James, 494 F.2d 1007, 1013-16 (D.C. Cir.), *cert. denied*, 419 U.S. 1020 (1974).

178. The recent Report of the President's Domestic Council Task Force on Drug Abuse recommended a focus on prosecution of the leaders of high-level trafficking networks as the most effective way to cut off drug supplies. The report stated that conspiracy cases are the only effective means for the law to reach these leaders since they "normally insulate themselves from *overt illegal acts* by delegating these acts to subordinates." 18 CRIM. L. REP. 2128, 2129 (1975) (emphasis added). If the leaders commit no overt illegal acts themselves then electronic snooping on their activities would provide no independent evidence of crime.

clandestine observation of a plant for the processing of illegal narcotics would yield useful evidence. But the strict particularity required prior to the issuance of an electronic snooping order would fully justify a conventional search and seizure. A clandestine method of intrusion would be necessary only to develop further information as to the nature and scope of the conspiracy without alerting the suspects to the surveillance. Electronic snooping would be no more useful for this purpose than electronic eavesdropping. Also, electronic snooping appears to be an ineffective technique for observation of actual drug sales to the users of the drugs. Evidence of such sales can be provided by the use of wired informers or undercover agents who purchase drugs with marked money.[179] Often sales take place with insufficient advance notice to permit the installation of electronic snooping equipment. Frequently, too, sales take place on the street or in other semi-public places where traditional camera surveillance can be employed,[180] even at night,[181] with sufficient advance warning to allow the installation of the equipment. Thus the unique ability of electronic eavesdropping to provide information vital to narcotics investigations finds no parallel in electronic snooping.

The primary justification for any clandestine information-gathering technique in law enforcement therefore appears to be its ability to uncover the full scope of a criminal conspiracy without alerting already known suspects to the existence of the investigation. Since any broad conspiracy of this type necessarily involves the extensive use of oral communications between the conspirators, interception of these communications is the primary investigative tool.[182] It follows logically that the only other area in which electronic snooping might be effective is in the investigation of small-scale or individual offenses, such as personal drug use, prostitution or a neighborhood poker game. In such cases electronic surveillance is unnecessary since there is no conspiracy whose scope is to be uncovered. The probable cause necessary for the issuance of an electronic snooping order would support a conventional search and seizure, which would be equally effective. Therefore, in the investigation of either large-scale conspiracies or individual offenses, electronic snooping would fail to satisfy the necessity requirement.

179. *See* United States v. Quintana, 508 F.2d 867, 872-73 (7th Cir. 1975).

180. *Id.*

181. See text accompanying notes 41-47 *supra.*

182. Electronic eavesdropping "has a well-established record of producing positive results against the veteran practitioners of organized crime." 18 CRIM. L. REP. 2082, 2083 (1975) (remarks of F.B.I. Director Clarence M. Kelley).

C. Application of the Balancing Test

1. Nature of the Invasion of Privacy

Electronic snooping clearly intrudes upon individual privacy to a greater extent than does electronic eavesdropping. During the surveillance the invasion of privacy by observation is continuous rather than limited to periods of actual communication as in the case of electronic eavesdropping. Electronic snooping is thus literally inescapable, even in the dark, whereas electronic eavesdropping can at least be avoided by maintaining silence.

In addition, the privacy interest invaded is significantly greater. Electronic snooping invades not merely the oral expression of thoughts but the intimate province of freedom from physical exposure of one's body to the view of others. An oral communication has already lost some of the privacy accorded to pure thought merely by the fact of communication to another person. Therefore no absolute expectation of privacy exists in any oral communication, because the listener can always inform the police of what he has heard.[183] But the expectation of privacy in activity performed in the absence of any known observation is *absolute*. The act of viewing such activity by clandestine means must be considered a more serious intrusion upon individual privacy and integrity than the overhearing of oral communications to other persons.

Finally, in its practical operation electronic snooping would unavoidably constitute a greater invasion of privacy than electronic eavesdropping. The application of minimization principles to the execution of an electronic snooping order would inevitably invade the individual's privacy to a greater extent than the corresponding search conducted by electronic eavesdropping.[184] This greater invasion of privacy would be unreasonable under the Fourth Amendment in the absence of correspondingly greater law enforcement justification.

2. Law Enforcement Justification

As discussed above,[185] there is no apparent necessity for electronic snooping in law enforcement because of the availability of electronic eavesdropping and other conventional investigative tools. While electronic snooping might provide corroborating evidence of crime it would not by itself enable the prosecution of criminals who presently escape prosecution because of the inability of law enforcement officials to gath-

183. United States v. White, 401 U.S. 745 (1971).
184. See text accompanying notes 148-156 *supra*.
185. See text accompanying notes 162-182 *supra*.

er sufficient evidence. If rather than to obtain direct evidence of crime, electronic snooping were to be used, for example, to identify the participants in a suspected meeting of organized crime leaders or other conspirators, less intrusive alternative techniques again could accomplish the same objective. Such techniques as visual surveillance outside of the premises, including methods for overcoming darkness or distance,[186] and conventional voice identification methods applied to the oral communications which could be overheard by a listening device authorized by Title III, should prove adequate for individual identification without resort to electronic snooping.

The other major argument in favor of legalized electronic eavesdropping is that because organized crime is making free use of the telephone in furtherance of its criminal objectives, wiretapping is a necessary law enforcement response in opposition to this "perversion of the telephone to criminal use."[187] The addition of electronic snooping to the police arsenal cannot be supported by this same justification. Undoubtedly criminals still commit murders, store stolen merchandise and grow marijuana plants in violation of the law within the confines of their homes or offices. Yet they do so not with the aid of television or any other new technological development which might justify a law enforcement response in kind, but behind the same four walls which have traditionally protected them from unwanted visual intrusions.[188] In the absence of any new development preventing or hindering the exercise of conventional search and seizure power, it is an insufficient justification for any new technique for clandestine intrusion upon indi-

186. See text accompanying notes 41-47 *supra*.

187. Sullivan, *Wiretapping and Eavesdropping: A Review of the Current Law*, 18 HASTINGS L.J. 59, 60 (1966). *See* THE CHALLENGE OF CRIME IN A FREE SOCIETY, *supra* note 168, at 200-01. "The marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission, and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its law-abiding citizens." United States v. United States District Court, 407 U.S. 297, 312 (1972).

188. Consider a California police chief's justification for the use of television in law enforcement insofar as it might apply specifically to electronic snooping: "Throughout the years, it has traditionally been the criminal who has first taken advantage of technological advances . . . . The automobile and the two-way radio are prime examples; law-breakers were the first to employ them, and the police then adopted their use *in self-defense*. But now police departments are taking the offensive in moving into new areas before the law-breakers. Our own use of closed-circuit television as an important law enforcement tool is a step forward in this direction. We're learning to use CCTV extensively to enforce the law before someone figures out a way to break the law with it." O'Brion, *VTR: New Lawman*, INDUSTRIAL PHOTOGRAPHY, Nov. 1971, at 26 (emphasis added).

vidual privacy to say that it should be used merely because it is available and is an easier or more convenient way to gather evidence of crime.[189]

The only remaining justification for electronic snooping seems to be that it would provide a videotape of a defendant's activities which, as a piece of physical evidence at a criminal trial, might have considerable influence on a jury. In addition to an informer's or undercover agent's testimony, physical evidence that has been seized, and the defendant's own words intercepted by a wiretap or bug, the jury could observe the private acts of the defendant on television. However, this use of electronic snooping completely ignores the constitutional requirement that conventional methods be *inadequate* to obtain the same or similar evidence. The necessity requirement must not be read as permitting the use of any technological improvement which produces more convincing proof of the same facts provided by other methods.

The law enforcement justification for electronic snooping is therefore clearly no greater than that for electronic eavesdropping, and indeed may be less compelling. Undoubtedly, however, the intrusion upon personal privacy inherent in electronic snooping is considerably greater than that resulting from electronic eavesdropping. A consideration of all the factors on both sides of the scales leads to the conclusion that the present justification for electronic snooping does not outweigh the degree of intrusion upon personal privacy occasioned by its use. By Fourth Amendment standards, electronic snooping must therefore be considered an unreasonable law enforcement tool under any circumstances.

VI. Conclusion

Prior to 1968 the propriety of legalized electronic eavesdropping had been the subject of a long and heated national debate.[190] Against claims of the need for electronic eavesdropping in the war against sophisticated criminals[191] opponents of eavesdropping objected that "we destroy exactly what we are seeking to preserve when we try to protect

189. "One must be careful to distinguish betweeen constraints on police conduct which limit effective police enforcement and those constraints which merely make effective police enforcement more burdensome.

. . . Duties of law enforcement officials are extremely demanding in a free society. But that is as it should be. A policeman's job is easy only in a police state." People v. Spinelli, 35 N.Y.2d 77, 81-82, 315 N.E.2d 792, 795, 358 N.Y.S.2d 743, 747-48 (1974).

190. *See generally Symposium: The Wiretapping-Eavesdropping Problem: Reflections on The Eavesdroppers*, 44 MINN. L. REV. 811 (1960).

191. *See* Berger v. New York, 388 U.S. 41, 61-62 (1967). See notes 167-169 *supra* and text accompanying.

democracy with essentially totalitarian tools."[192] The debate finally resulted in a national consensus, expressed through the Congress, that the usefulness of electronic eavesdropping in certain areas of law enforcement outweighed the risks resulting from its indiscriminate nature and potential for abuse when it was permitted only under conditions of strict judicial control.

Now, another technological development for surreptitious surveillance of individuals has emerged. Electronic snooping carries the threat that every physical act of an individual may be subject to observation by an unseen viewer through the medium of an electronic eye. If allowed to go unexamined, the use of electronic snooping devices might eventually become so widespread, as have the tools of electronic eavesdropping,[193] that a true feeling of security from clandestine visual intrusions may become a thing of the past.[194] The psychological fact, even if not the physical reality, would be the arrival of the world of 1984, because " 'Nineteen Eighty-Four' is largely a state of mind; for many, the appearance of repression has the impact of reality."[195] Today "anyone can protect himself against surveillance by retiring to the cellar, cloaking all the windows with thick caulking, turning off the lights and remaining absolutely quiet."[196] With the advent of electronic

192. Williams, *The Wiretapping-Eavesdropping Problem: A Defense Counsel's View*, 44 MINN. L. REV. 855, 856 (1960).

193. *See, e.g.*, O'Toole, *Harmonica Bugs, Cloaks, and Silver Boxes*, HARPER'S MAGAZINE, June 1975, at 36 (describing the current state of the art of some eavesdropping devices); *The Ways and Means of Bugging*, TIME, May 28, 1973, at 28. Despite Title III's ban on the advertisement and sale of eavesdropping devices, 18 U.S.C. § 2512 (1970), devices easily adapted to surreptitious listening are still freely advertised. *See, e.g.*, PLAYBOY, Nov. 1975, at 223: "MICRO MINI MIKE. WIRELESS. Among world's smallest. Improved solid state design. Picks up and transmits most sounds without wires through FM radio up to 300 ft. Use as mike, music amp., babysitter, burglar alarm, hot line, etc. For fun, home and business. Batt. incl. Money back guar. . . . Only $14.95 plus 50¢ Post and hdlg."

194. For example, because of his legal representation of politically sensitive causes, Stanford Law Professor Anthony G. Amsterdam admits that he no longer has any actual expectation of privacy in his private conversations. Amsterdam, *supra* note 75, at 384. Justice Douglas wrote that he was "morally certain" that the Supreme Court conference room had been bugged. Heutsche v. United States, 414 U.S. 898 (1973) (denial of bail motion) (Douglas, J., dissenting). Representative Ronald V. Dellums of California recently revealed that a wiretap of his Berkeley office phone was discovered in 1972 and that he now operates under the assumption that both his Berkeley and Washington offices are bugged. San Francisco Chronicle, Oct. 10, 1975, at 6, col. 1.

195. Miller, *The Right of Privacy: Data Banks and Dossiers*, in ROSCOE POUND—AMERICAN TRIAL LAWYERS FOUNDATION, ANNUAL CHIEF JUSTICE EARL WARREN CONFERENCE ON ADVOCACY IN THE UNITED STATES, PRIVACY IN A FREE SOCIETY 72, 75 (1974).

196. Amsterdam, *supra* note 75, at 402.

snooping, a person wishing to assure the privacy of his actions from visual observation will have no absolute protection even by resort to these extreme measures.

Fortunately, our society is presently in a position to deal effectively with the problems posed by electronic snooping. We have experienced the controversy over electronic eavesdropping and have observed the results of the implementation of a strictly supervised system for its limited use.[197] We have also become aware of the technology of electronic snooping while it is still in its infancy. Informed, effective decisions are therefore possible. No currently available evidence indicates that electronic snooping would fill a law enforcement need caused by the inadequacy of other presently available investigative techniques. Thus the considerations which prompted acceptance of electronic eavesdropping as a law enforcement tool are not present to justify the use of electronic snooping even under restrictions similar to those imposed by Title III. In balancing the legitimate needs of law enforcement against the personal interests invaded, a court faced with a challenge to evidence obtained by electronic snooping, whether or not authorized by court order, should declare the technique unreasonable per se under the Fourth Amendment.

The present conditions of rapid technological development demand that the impact of new technology upon individual privacy be evaluated and controlled before its use becomes widespread, for failure to do so would eventually "dim the right [of privacy] almost to the point of extinction."[198] Because considerable time may pass before judicial consideration of electronic snooping, legislation should be enacted to prohibit the use of electronic visual surveillance techniques when such use intrudes upon an individual's reasonable expectation of privacy from such surveillance. Strict enforcement and control procedures should be included in the legislation. Only in this way will the citizen's right to privacy be *affirmatively asserted* before electronic snooping technology advances beyond manageable proportions.

The continuing evolution of highly sophisticated electronic devices clearly demonstrates the dangers inherent in their automatic adaptation to law enforcement use solely because of their availability. Those who would utilize new methods of clandestine intrusion upon individual privacy must bear the heavy burden of justification for such use. In the

197. For contrasting views on the results, *compare* Schwartz, *Six Years of Tapping and Bugging*, 1 Civ. Lib. Rev. 26 (1974) *with* Cranwell, *Judicial Fine-Tuning of Electronic Surveillance*, 6 Seton Hall L. Rev. 225 (1975).

198. Hufstedler, *supra* note 13, at 550.

case of electronic snooping this burden simply has not been met. The farsighted words of Justice Brandeis, penned at a time when electronic eavesdropping was similarly in its infancy, evoke the present danger:

> Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.[199]

199. Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).

[From The Privacy Report, Issued by Project on Privacy and Data Collection/ American Civil Liberties Union Foundation, No. 10, May 1974]

TV: A Two-Way Street

You probably wouldn't regard your television set as a privacy threat. If it bothers you, you can always turn it off. But cable television, about the most heralded technological revolution in 50 years, promises to change all of that.

Cable is many things. For most Americans, cable is a method of communication using wires rather than the broadcasting wave lengths employed by over-the-air radio and TV. This difference allows cable TV to transmit many more channels than conventional broadcasting and to provide clear signals to remote areas.

Thus, the early discussions about cable TV involved squabbles over regulating and enfranchising local systems and over the significant First Amendment aspects of a system that promised to enhance opportunities for free expression—if not captured right off by monopolistic interests. (See "An ACLU Guide to Cable Television" by Fred Powledge, 1972)

Cable television is a two-way street. Technological advances now allow for interactive (two-way) cable television. Now, writes Ralph Lee Smith, author of *The Wired Nation*, "There can come into homes and into business places audio, video, and facsimile transmissions that will provide newspapers, mail service, banking and shopping facilities, data from libraries and other storage centers, school curricula and other forms of information too numerous to specify. In short, every home and office will contain a communications center of a breadth and flexibility to influence every aspect of private and community life."

Experimental two-way systems, allowing images and messages to travel to and *from* the home, have been launched in a dozen American communities. The implications for the subscriber's privacy are immense.

In Rossmoor's Leisure World, Mesa, Ariz. senior-citizen residents not only can't turn off their TVs, but their TVs can be turned on without their knowledge or control. Every new home is wired for two-way TV, including fire detector, emergency call alarm, and a burglar alarm for security purposes. Police or firemen can be notified immediately of emergencies. "Once you've done that," says James Richards of the United Church of Christ Office of Communications, "you've set the precedent for observing a home." Burglar and fire monitors by cable could automatically turn on to view inside the residence in the event of an emergency—or in the case of a curious snooper at "the headend" of the two-way system—even if the resident is not home. Such a turn-on violates Federal Communications Commission recommendations.

Other proposed uses of cable TV raise privacy issues:

Shopping for merchandise, theatre tickets or library materials from the living room by dialing a code after scanning offerings on the screen. A computerized record of such choices could easily be kept, and in some pilot projects subscribers are powerless to prevent this. Some experts have proposed destruction of "data trails" or scrambler devises to assure anonymity. Without such assurances, subscriber choice of chan-

nels or purchases could be available electronically as a salable commodity, for surveillance, or for investigation.

Voting or registering opinions by cable. Cable transmissions can be intercepted surreptitiously, like telephone communications, and so devices to assure a secret ballot must be developed. El Segundo, Calif., site of a 20-home cable test, has legislated to prohibit disclosure of data about individual cable users and to prohibit tabulations of religious, political or social views of users. (Resolution 2425, Feb. 7, 1972).

Home study by cable TV for part-time, handicapped or remote students. Also out-of-home meter reading by utility companies. Once again, the possibilities of snooping are endless.

This is not to say that your conventional one-way, over-the-air television can't invade your privacy too. One example is "subliminal perception" advertising like the pre-Christmas commercial during which the message "Get It" was flashed on the screen for a split second four times. Ad men say the technique actually induces viewers to buy the product, but the FCC calls the practice "deceptive" and "contrary to the public interest." (39 Fed. Reg. 3714, Jan. 29, 1974).

Business and government interoffice communications. The Mitre Corp., of McLean, Va., is studying for the Law Enforcement Assistance Administration possible uses of cable, closed circuit and video tapes in the criminal justice system whereby, for instance, expert witnesses could save time by testifying from their offices and line-ups could be relayed to out-of-state police departments. Urban relatives could also visit by TV with inmates in rural prisons. Mitre is the sponsor of a demonstration project in Reston, Va. that provides computer-generated information that can be selectively received and displayed on a standard TV set. Transmission to the home is by conventional one-way cable and from the home to the computer by personal telephone.

TV games or "interaction" with the computer. Persons could play chess with a computer by cable TV, perhaps, or ask for advice or talk back to avoid loneliness or get the computer's help on what to do until the doctor comes. If all of this information is stored and made retrievable, many citizens will be scared away from cable TV's benefits.

This new world of communication could be opened to the consumer for less than the cost of a $200 home terminal, but without more attention to privacy safeguards the price will be much higher for those who value privacy.

[From The Privacy Report, Issued by Project on Privacy and Data Collection/ American Civil Liberties Union Foundation, Volume IV, No. 1, August 1976]

Private Police in America: The Private Security Industry

(By Richard M. Hartzman [1])

Judging from the number of pulp detective novels published each year and the endless stream of television detective serials, the private eye has become an archetypal American folk hero. He works on his own, is either engagingly handsome or has winning eccentricities, and

[1] Mr. Hartzman is a member of the New York and Colorado Bars. He has been active on behalf of the rights of Soviet Jewry, and is currently involved in legal efforts to enforce stringent air pollution standards in the operation of public utilities.

overcomes enormous obstacles to unravel a murder or bust a drug ring. Since our hero's goal is legitimate and he champions innocent victims, an occasional assault, illegal entry, theft of private papers, use of deception to gain information, even extortion, are viewed with little trepidation.

The media delude the public on two counts. The first is that many of the illegal practices of private detectives are justified, even commendable. They are not, but our legal system has developed insufficient controls to curb them. The second is that everyone's favorite detective is somehow typical. Not only does the solo private eye account for a tiny proportion of the total number of private investigators in the country, but investigators as a whole constitute only 10 percent of the huge private security industry.

The development of police forces is a universal feature of advanced industrial societies. In the United States this has occurred to a large extent in the private sector. The functions and practices of private police or private security forces are similar to those of public police forces, but they are not subject to the same measure of public control, nor to the same constitutional restraints.

WHO'S WHO IN THE INDUSTRY

Estimates of the number of private security personnel vary from 300,000 to 1 million. About 90 percent are guards, watchmen, or patrolmen. Investigators, detectives, and undercover agents make up the rest. A recent article in the New York *Times* claimed that there are 100,000 private guards in New York City alone. A study conducted by the Rand Corporation for the Law Enforcement Assistance Administration (LEAA) estimated that in 1967 there were 4280 detective agencies and protective service establishments nationwide. The biggest firms dominate the industry and have more employees than most large metropolitan police forces.

"In-house" personnel, employed directly by a single business, manufacturer, institution, or individual, make up the greater portion of private security forces. The remainder are "rent-a-cops" employed by contract security agencies.

The dollar volume of private security business has been estimated at $5–$10 billion a year. Equipment expenditures for items such as armored cars, alarms, and closed-circuit television are over $800 million a year. Over the past decade the private security industry has grown at an annual rate in excess of 10 percent, a rate not appreciably affected by the 1973–75 recession. With approximately 475,000 public police nationwide, the number of private police personnel and total expenditures for private police are comparable to, if not greater than, the figures for public police forces.

What was probably the world's first private detective agency was started in Paris in 1832 by Francois Vidocq, after two decades of working for the Paris police force. Private police in the United States had a sordid beginning. In response to the abolitionst movement, a network of private investigators came into being in the North, paid by slaveowners to track down escaped slaves and inform on those who harbored them.

Allan Pinkerton opened a private detective agency in Chicago in 1850. In the early years his agency worked on criminal cases not handled by local police departments, which were hampered by jurisdictional limits, incompetence, or corruption. Until the advent of the FBI, Pinkerton's functioned virtually as a national police force. It was Pinkerton who developed the rogue's gallery, the model for what has become the FBI's National Crime Information Center.

Railroad, mining, and industrial police forces were also established in the nineteenth century. The latter two were notorious for fighting labor organizers and, after World War I, suspected radicals. Informers, undercover agents, and agents provocateurs were freely used. After a series of exposés and congressional hearings, labor spying was prohibited in 1936 by the Wagner Act. That did not end the practice, however.

The explosive growth of the private security industry occurred after World War II, partly in reaction to increasing commercial and industrial theft. Today, private security forces can be found in such diverse settings as retail, financial, and industrial establishments, hospitals, hotels and apartment houses, educational, recreational, and transportation facilities, and even some public agencies.

The largest and oldest security firm in the country is Pinkerton's, Inc. In 1974 Pinkerton's had a work force of over 38,000 and revenues of $193 million. This compares with revenues of $64 million in 1964 and only $4 million in 1944. Its annual report lists over a dozen types of security and investigative services, among which are surveillance, applicant and fraudulent claims investigation, developing evidence for civil litgation, and solving inventory shortages. The term "private eye" derives from Pinkerton's old trademark, "The eye that never sleeps."

William J. Burns International Detective Agency, Inc., had a work force of 39,000 and revenues of $153 million in 1973. It was founded in 1909 by William Burns, a former Secret Service investigator, when he was awarded a contract for security operations by the American Bankers Association. Burns provides criminal investigative service for the defense of accused persons—a service Pinkerton's no longer offers—as well as "management control services": inventory loss, pilferage, theft, fraud, falsification of records, poor employee morale, neglect of machinery, waste of manhours and materials, working conditions, safety hazards, etc.

The Wackenhut Corporation was founded only in 1954. By 1974 it had a work force of over 18,000 and revenues of $94 million. In 1969, 14 percent of its business was through direct government contract with agencies such as the AEC and NASA. (Wackenhut is only one of several private contract agencies to do business with the federal government, despite the Pinkerton Law prohibiting the employment of detective agencies by the government.[2] Wackenhut also provides security for airports and for the Trans-Alaska Pipeline System.

Other giants of the industry are Walter Kidde and Co. (Globe Security Systems), specializing in the provision of uniformed guard serv-

[2] The Pinkerton Law, 5 U.S.C. § 3108, was enacted in 1893 after congressional hearings held partly in response to the behavior of Pinkerton agents during the Homestead Strike. But a 1946 ruling by the U.S. Comptroller General declared that (1) a subcontract for private guard services by an independent contractor of the government, and (2) procurement of services from "protective" as distinguished from "detective" agencies, are permitted. Because of this narrow interpretation, the law is generally ignored.

ices and airport security, and the Wells Fargo Security Guard Group of Baker Industries, Inc. Baker, besides providing guard services, is the nation's second-largest supplier of central station alarm and armored car services. Brink's, Loomis, and Purolator are the other major armored car firms. The four account for over 75 percent of this business in the country. American District Telegraph Co., which began as an offshoot of Western Union in 1854, is by far the largest provider of central station alarm services, with 1969 revenues of over $97 million.

Some of the larger companies have offices worldwide, making possible worldwide private police organizations. It is these giants, and their numerous smaller imitators, rather than TV's rash of ingratiating heroes, who typify the private security industry.

RETAIL SECURITY

The purpose of retail security is to prevent or minimize losses from theft, burglary, pilferage, credit card fraud, and forgery, and similar problems common to mercantile establishments. It is aimed at both customers and employees. A security department, whether in-house or contract, is expected to cut down on losses and at the same time avoid incurring liability for wrongful actions. There is further economic incentive to install retail security systems because discounts on crime insurance are often given to establishments which use them.

Surveillance in stores is commonplace. Television cameras and well-placed convex mirrors abound. Some stores have uniformed guards, although the more effective practice is to use plainclothes floor detectives trained to spot shoplifters. Pillars and two-way mirrors conceal guards. Hidden catwalks and observation posts may be constructed in ceilings, as in the casinos in Las Vegas. Spotters and honesty shoppers are used to check on employees. Undercover agents may be employed as clerks or cashiers. As in regular police work, the use of undercover agents presents the potential for entrapment.

Surveillance, which may not be objectionable in the open areas of a store, becomes obnoxious when employed in the two areas most likely to be used to conceal stolen goods—fitting rooms and restrooms. Even though they are public facilities, these are places where one ought to have an expectation of privacy. And the possibility of observation by members of the opposite sex while changing clothes or going to the bathroom is an obvious intrusion on traditional and deeply held notions of privacy. The most-used surveillance devices in these areas are two-way mirrors, mirrors on ceilings, louvered doors, grated air vents, and observation posts in ceilings.

Surveillance practices have recently come under increasing criticism and some limitation. California made it a misdemeanor to use two-way mirrors in restrooms, toilets, locker rooms, fitting rooms, and hotel and motel rooms. Cal. Penal Code § 653(n). In *People* v. *Metcalf*, 98 Cal. Rptr. (Ct. of Appeals, 1971), the court declared that this statute expressed a public policy against such clandestine surveillance, and suppressed a police officer's testimony as to matters seen through a louvered door. In a lower court decision in New York City, it was held that individuals have a "reasonable expectation of privacy" in closed fitting rooms, and the court suppressed evidence gained from the ob-

servation of the defendant in a fitting room in Gimbels department store. In that case the security person was a "special patrolman" licensed by the city and appointed by the police commissioner. The category of special patrolman was created by local ordinance and granted powers greater than those of the ordinary private security officer or the average citizen. Hence, the Fourth Amendment was held to apply. But had the security person not been specially deputized, the evidence, although obtained through the same means would have been admissible. *People* v. *Diaz*, Crim. Ct. of N.Y.C., Docket No. N/534102/75, December 4, 1975.

As clandestine surveillance practices come under attack, many stores are substituting more open methods, such as the use of checkers at the entrance to fitting room areas or the placing of special sensory tags on clothing. But the use of surreptitious surveillance in fitting rooms is not a dead practice.

DETENTION AND ARREST

Private police, with just a few exceptions, do not have the legal status of peace officers. Neither do they have any greater power of arrest or search than the ordinary citizen. One exception is that category of private security personnel who are deputized or commissioned by a public agency, often a city police department. These "special police" work in department stores and other establishments in New York, St. Louis, Miami, and some other cities. They have the same power of arrest as a public police officer, but generally only while on duty and on the premises on which they are employed. Some state courts, as in the Gimbels case, have placed these special police under constitutional restrictions similar to those which govern the conduct of public police, and such officers, like the public police, may be subject to lawsuits for the violation of individuals' civil rights under color of law, 42 U.S.C. § 1983. Another exception to the limited legal powers of private police occurs when a public police officer moonlights in the private security business. He carries his power of arrest with him at all times.

The ordinary citizen's power of arrest varies somewhat from state to state. Generally, a person can make a citizen's arrest when a felony is committed in his presence, or when he knows a felony has been committed outside of his presence and he has reasonable grounds to believe that the person he arrests committed the crime. A citizen can make an arrest for a misdemeanor only if it is committed in his presence. Thus, in most shoplifting cases, the store detective must see the articles taken in order to make an arrest. As to misdemeanors, no mistake is allowed, and an error can lead to a lawsuit against the store for false arrest. Judgments in such cases may run into thousands of dollars. Recently, a jury in New York City awarded $1.1 million in a "wrongful detention" lawsuit in which a suspected shoplifter was detained by store security guards, turned over to the police, tried, and acquitted after ten minutes of jury deliberation.

Because the private police power of arrest is so limited, most states have created a special statutory privilege of detention as a means of dealing with suspected shoplifters. Detention is allowed upon "probable cause" for a "reasonable time" and in a "reasonable manner." Some form of interrogation and search is generally permitted. State

courts have attempted to define what is meant by "probable cause" in this context, but it remains a vague term. Standards for search and interrogation are essentially undeveloped. The constitutional safeguards concerning arrest, search and seizure, and interrogation do not apply except where special police are involved. Evidence which private police obtain by methods prohibited to the public police may be turned over to the public authorities and used in criminal prosecutions.

Detaining a suspect without probable cause, holding beyond a reasonable time, or trying to coerce a confession can lead to a civil action for false imprisonment or wrongful detention. A defamation action may be brought if a suspect is questioned in public and false accusations are made. Although defamation actions are difficult to litigate, false imprisonment and wrongful detention suits are fairly common, and often successful.

If a guard does not have grounds for an arrest or detention, he can still use "reasonable force" to regain possession of the article. The usual practice is to allow the shoplifter to leave the store, and then forcibly retrieve the goods and let the person go free. Most stores would just as soon avoid a criminal prosecution, and this mode of action at least prevents the loss. Obviously, such practices set up a situation in which confrontation and violence are possible. Assault complaints against security forces are common. In some circumstances, security personnel can be criminally prosecuted.

INTERROGATION

The lack of standards for interrogation by private security officers leaves this procedure particularly open to abuse. Although there is some judicial precedent for excluding coerced confessions obtained by private police in criminal prosecutions, *People* v. *Frank*, 275 N.Y.S. 2d 570 (Sup. Ct., 1966), Miranda warnings are not required.[3] It is common for a suspected shoplifter to be told that the police will be called unless he signs both a confession and a release waiving all grounds for suit against the store. The suspect is often denied the opportunity to telephone a friend, relative, or lawyer. Minors are often threatened that their parents will be informed. The suspect may be held for a considerable period of time until a confession is signed, and then let go without prosecution. Many innocent people are sufficiently terrified or concerned about avoiding further trouble with police or family that they sign a confession in hopes that the incident will be closed.

The private police officer, through his own distinctive privilege of detention, in effect enforces an alternative system of private justice, virtually unrestricted by the constitutional safeguards of the Fourth and Fifth Amendments which are guaranteed to individuals in the enforcement of public justice. But a strong argument can be made that constitutional guarantees should apply, for the private police officer ultimately derives his special privileges from the state. And on purely practical grounds, as we shall see, the effects on future employment

[3] Upon detaining a suspect for questioning, a public police officer must warn him that he has the right to remain silent, that anything he does say may be used against him, that he has the right to a lawyer, and that if he cannot afford a lawyer, one will be obtained for him. These are called Miranda warnings, as established by the Supreme Court decision in *Miranda* v. *Arizona*, 384 U.S. 436 (1966).

for the individual who is detained and questioned by a private officer may not be very different from the effects of a similar experience at the hands of the public police. At present, individuals have only private remedies, in the form of civil suits, to try to obtain redress after the fact, an expensive, often embarrassing, and difficult method of protecting one's rights.

RETAIL PROTECTIVE ASSOCIATIONS

In many cities the suspected shoplifter is not forgotten by this private system of justice. A record of the incident and copies of any confession and release are filed with the local retail protective association. A prime example of such an organization is New York's Stores Mutual Protective Association (SMPA), founded in 1918 by Gimbels, Lord & Taylor, Abraham & Strauss, and Macy's. SMPA had over 500,000 files on individuals involved in shoplifting incidents by 1960. Files are also maintained on employees allegedly involved in thefts and frauds. If a person applies for a job at a member store of SMPA, and if SMPA has a file on him, he is essentially barred from local retail employment. It does not matter if the report is based on erroneous information, a coerced confession, or an incident which occurred when the person was a juvenile. These records are often made available to credit reporting agencies, which disseminate them widely to prospective employers.

Federal and state Fair Credit Reporting Acts are applicable to the activities of retail protective associations, but they have many loopholes. The New York Civil Liberties Union is attempting to amend that state's FCRA to close one loophole, with a prohibition on the collection and disclosure of information regarding conduct for which a person could have been treated as a youthful offender under the penal law. Thus, dissemination of information on juvenile shoplifting incidents would be forbidden.

Another improvement would be to require some variations of a Miranda warning when a shoplifting suspect is detained and interrogated. One element of the warning would be to apprise the suspect that a confession will be placed on file at the retail protective association, whether or not criminal charges are brought, and reported to prospective employers in the future.

The following case illustrates a common situation arising from the practices of retail protective associations, and suggests one possible kind of remedy. In early 1976 the Massachusetts Attorney General took action under that state's FCRA against a department store which was using Boston's Protective Services, Inc. (PSI). The store had violated the act by failing to notify a new employee that a pre-employment check would be made, and then firing her without telling her that the dismissal was based on a PSI report stating that she had been suspected five years earlier of attempting to shoplift three pantsuits. She had denied the charge, paid for the clothes, and was not prosecuted. The department store agreed to discontinue its use of PSI, and as a consequence PSI closed down after fifteen years of operation.

That arrest information is freely circulated by credit reporting agencies is well known, but it may not be so widely known that many

"criminal background" reports are based on run-ins with a private law enforcement system which can detain people and obtain their confessions with virtual freedom from restriction. FCRA procedures for expunging erroneous information do not really help: reports of such detentions and confessions are not erroneous.

The procedures described here for the apprehension, detention, interrogation, and reporting of suspected shoplifters are used also for handling incidents of employee theft. It is common for an employee to be questioned and accused of theft by his employer's private security force, summarily dismissed but not prosecuted, and then barred from future employment because of a report of the incident maintained by a retail protective association or credit reporting agency.

PRIVATE INVESTIGATION

Information gathering is the primary function of private investigative agencies. Investigators engage in pre-employment checks, background checks of insurance and credit applicants, undercover work to detect employee theft, and investigation of insurance claims. They may also aid attorneys in criminal defense work and personal injury cases. Marital investigations, once an important aspect of the business, are declining as divorce laws are liberalized.

Where fraud, theft, or pilferage is involved, private and public police may work together. They may refer cases to each other or cooperate in the apprehension of a suspect. They may exchange information, sharing in the intelligence gained through their respective networks of informers. Private police may lend investigative and surveillance equipment to public police. Private police can also provide a means for public police to evade or subvert constitutional restrictions and rules of procedure.

Privacy problems involved in credit and insurance investigations and reports have been well covered in the literature. Less publicized is the fact that when private security firms such as Wackenhut and Burns engage in criminal investigative work as well as pre-employment checks, they maintain files on the people they investigate. Wackenhut was reported to have 3 million files on individuals in 1967 and to be adding 10,000 per week. When these files are made available by private security firms to their clients, the provisions of federal and state Fair Credit Reporting Acts are usually applicable. But the flimsiness of the protections and restrictions imposed by these laws is all the more evident when the files contain indications of suspected criminal activity based only on information gathered by the free-wheeling practices of private investigators.

ELECTRONIC SURVEILLANCE

Federal and state laws prohibit tapping and "bugging" by private individuals of wire and oral communications, except in certain circumstances where one party to the communication has given consent. Federal law prohibits the manufacture, distribution, possession, and advertising of devices "primarily useful" for "surreptitious interception of wire or oral communications." 18 U.S.C. § 2512(1). Evi-

dence obtained through illegal private eavesdropping is generally excluded by federal and state law from use in criminal or civil proceedings. In addition, illegal tapping or electronic eavesdropping constitutes the tort of invasion of privacy in virtually all states, and the placing of a bugging device on private property can also be grounds for a trespass action.

With this wide array of legal sanctions, one might expect that the use of electronic surveillance devices by private persons would be rare. Such is not the case. Last year the National Wiretap Commission conducted a random check of 115 private detective firms. It found that 42 of these either offered illegal wiretap services themselves or advised how such services could be obtained. Many firms were also willing to provide bugging systems. "Debugging" services—clearing rooms of hidden microphones and other electronic surveillance devices—were offered by 71 firms.

So numerous are the devices available for electronic eavesdropping, and so sophisticated the technology, that many forms of eavesdropping do not appear to fall afoul of existing laws. Moreover, the statutory one-party-consent exception is extremely vague and has been ambiguously interpreted by the courts. The use of one-party-consent eavesdropping in private investigations is therefore commonly thought to be permissible. Most people assume they have the right to bug their own telephones to catch conversations by errant spouses or children. Long-range transmitters positioned in public places involve no breaking and entry to install, and therefore may appear to be legal. Closed-circuit TV and eavesdropping equipment intended as security devices may be used by employers to pick up conversations among employees. In fact, such systems are frequently installed as standard equipment in new buildings. It is a widespread practice for employers to check up on their employees by monitoring company phones to overhear employee-customer conversations, unknown to the customer and often to the employee as well. Eavesdropping devices—miniature microphones, transmitters, recorders, and the like—are freely available on the market for legitimate use, and so too are the components from which a do-it-yourself eavesdropper can construct his own equipment.

With the barrage of technology and propensity for snooping, effective measures designed to curb private surveillance practices are difficult to conceive. Stricter enforcement of existing criminal sanctions may have a deterrent effect. More effective regulation of private detective firms, and the mandatory and permanent revocation of licenses for engaging in illegal wiretapping and bugging (already provided for by some states) might also bring some improvement. Consideration should also be given to a total ban on all bugging and monitoring by private persons, and a ban on all eavesdropping by one-party consent.

PHYSICAL SURVEILLANCE AND SEARCHES

Physical surveillance—"shadowing"—and the use of cameras and radio-transmitted "beeper" signals on automobiles or in doorways are frequently employed in the investigation of insurance and negligence claims and divorce cases. A number of state courts have found that certain surveillance practices are an unreasonable invasion of

privacy and have awarded damages to the victims. Overzealous shadowing, shadowing which is made obvious to neighbors, peeping in windows, and snooping around a house have all been held "unreasonable."

Related to the problem of surveillance is the search of private property. Private police have no power to conduct searches without consent. If an illegal search and seizure has been conducted, tort recovery might be based on a theory of trespass, conversion,[4] or invasion of privacy. In some states, such as Georgia, courts have held that an illegal search, even when the victim is not present, constitutes an invasion of privacy.

But tort recovery for illegal surveillance or search and seizure is a haphazard remedy. The victim may not know of the search or surveillance. If he does, he may be unaware that it is unlawful. If the information or material uncovered is sensitive, the victim may not want it further publicized in a legal action. Criminal prosecution for trespass or breaking and entry has been just as ineffective.

Evidence obtained through illegal surveillance or search and seizure by private police is admissible in civil actions and in criminal actions where there was no collusion with public police. The distinction between private persons and public police officials in the application of the exclusionary rule was made by the U.S. Supreme Court in *Burdeau* v. *McDowell*, 256 U.S. 465 (1921). The rationale for this distinction is doubtful in light of subsequent developments, and it would seem that the application of the exclusionary rule to evidence illegally obtained by private police, if not all private individuals, would create a significant deterrent to some of the more flamboyant illegal practices in which private investigators engage.

ACCESS TO INFORMATION

It is freely admitted by private security executives that private security firms have access to records of the public police even when local law or policy forbids it. In addition, private investigators make extensive use of police blotters and court records, and can often gain access to the records of credit card companies, hospitals, insurance companies, banks, schools, telephone companies, and many government agencies. Public police officers who moonlight in private security have even easier access to police records and other supposedly restricted information sources than do ordinary private investigators.

Where access is legitimate, private investigators have special know-how in the methods for obtaining records. Where access is prohibited, restrictions may be flouted by impersonation, by developing inside contacts through a "buddy system," or by bribery. A diligent and unscrupulous investigator can compile astonishingly complete dossiers on individuals.

Tort remedies, such as defamation and invasion of privacy, and Fair Credit Reporting statutes generally do not act as a restraint on private investigators' access to sources of information. Legal sanc-

[4] The tort of conversion is defined generally as the wrongful interference with the personal property of another. Wrongfully acquiring possession, unauthorized removal, wrongfully transferring possession, refusal to surrender possession, destruction, alteration, or wrongful use of personal property may all constitute conversion under specific circumstances.

tions—where they exist—against unauthorized access to confidential private or governmental records are so far little used, and in many instances not especially onerous.

A case which occurred in Denver in 1975 suggests a kind of remedy which could be highly effective if used vigorously. After Factual Services Bureau, Inc., had managed to obtain confidential hospital records, Colorado's Secretary of State revoked Factual's business license, and employees of Factual and the hospital were indicted for wrongfully obtaining the records.

CAMPUS SECURITY

In normal times, college and university campus security forces are engaged primarily in keeping intruders off campus, guarding dorms, issuing parking tickets, and detecting fires, theft, and vandalism. In times of political tension, such as the McCarthy and Vietnam War eras, they may move into the field of political surveillance and control of demonstrations. During these periods, public and private police engage in parallel activities, both independently and in close cooperation with each other.

The involvement of campus security personnel in drug investigations and searches is also a continuing problem.

In a study of campus security operations, Seymour Gelber found that 55 percent of private colleges and 76 percent of public colleges use undercover agents. Students are frequently used to report on their fellows; informers are also recruited from maids and resident advisers in dormitories.

When campus police engage in political surveillance and maintain files on students who participate in political activities, there are threats not only to privacy but also to the First Amendment freedoms of expression and association. There are essentially no legal standards as to what, if any, political surveillance on college campuses is acceptable, although at least one court, in California, has ruled that undercover campus surveillance, when carried into the classroom itself, is a violation of the First Amendment rights of both students and professors. *White* v. *Davis*, L.A. 30348, Super. Ct. No. C–32177 (March 24, 1975).

With the current campus calm, little attention is being paid to this problem. But the next time college campuses face political turmoil, the issue will again arise. The lessons of Kent State must not be lost. Extensive use of undercover agents at Kent State helped create the atmosphere in which the violent confrontations and killings of 1970 were possible.

TRAINING

The Rand study describes the typical private guard as an aging white male, 40 to 55 years of age, with little education beyond the ninth grade, usually untrained and very poorly paid. The typical private investigator or detective is a white male, 36 to 47 years of age, has completed high school, and has several years experience in private security. Retired police officers often find a second career in private security, usually as investigators or in security management.

Rand conducted a survey of private security personnel and found that less than half knew their arrest powers are no greater than those

of an ordinary citizen, and only 22 percent knew under what conditions an arrest is legal. Ignorance of the criminal law was common. "For example, 31 percent believe that it is a crime if someone calls them a pig."

The great majority of private security workers receive less than two days of training. It is not unusual for a newly hired guard to be issued a gun without receiving any firearms training. Few jurisdictions have training requirements set by statute or administrative regulation. Notable exceptions are St. Louis, which requires a three-day course to obtain a watchman's license, and Ohio, which requires a 120-hour course in order to qualify for a private police commission. However, in Ohio the employees of private security firms whose owners are commissioned may perform the same functions but need not themselves be commissioned.

The meagerness of the training for a private police career contrasts sharply with public police training requirements, which ranged from 72 to 400 hours in thirty states in 1971. It is ironic that licensed occupations with much less impact on our lives require more training. Many states demand 1000 hours or more of course-work for a barber's or beautician's license.

The Rand researchers reported a consensus among security executives that more training is needed, but that cost and price competition prevent any voluntary expansion of training courses. The answer to these arguments is a statutorily mandated training program applicable to all private security personnel.

The Rand study recommended a minimum initial accredited training program of at least 120 hours for all private security workers, with credit granted for prior law enforcement experience. An additional mandatory retraining program of at least two days per year was also recommended. The report urged a separate program for each job category, and examinations for all trainees. The recommendations specified the subjects to be taught for each type of security work, ranging from legal principle and investigative techniques to such practical subjects as first aid and alarm systems. All personnel carrying firearms would be carefully screened and required to complete an accredited firearms training course.

The response to the Rand recommendations was outrageous. Following publication of the study, LEAA in 1972 created a Private Security Advisory Council with representation from public law enforcement, business, industry, state criminal justice planning agencies, local government, and all segments of the private security industry. The Council eventually produced a "Model Private Security Licensing and Regulatory Statute." It provides for the licensing of contract security companies, but not investigative agencies or in-house security forces, and the registration of armed private security officers. A licensee must have a certain amount of experience or pass an examination. The statute is silent on the scope of examination, and there are no training requirements. Registrants must pass an examination after an 8-hour general training course. The statute would also require a firearms course and an annual refresher course. There are no training requirements for unarmed guards or for investigators.

LICENSING AND REGULATION

After a survey of state and local laws, the Rand researchers concluded that "licensing and regulation of the private security industry

at the state level is characterized by a lack of uniformity and comprehensiveness," and that no state has an adequate regulatory scheme.

As of 1975 nine states did not regulate the private security industry at all, although a few localities within those states had some regulation. Where there is licensing and regulation, it is aimed at businesses, not activities. Thus, no state has mandatory regulation of in-house guards or investigators, although some localities do. Surveillance consultants who provide services only to security firms escape licensing requirements. Grounds for denial or revocation of a license are vague or inadequate. Provisions for monitoring practices, investigating abuses, and handling complaints, bond claims, or court proceedings against licensees or their employers are generally inadequate. Employees of private security firms do not themselves need licenses or permits, and weapons regulation varies widely.

Rand made a number of serious proposals for improved licensing and regulation. It is enlightening to compare these with parallel provisions of the model statute prepared by the Private Security Advisory Council. What the chart makes obvious is the attempt by the private security industry to protect itself and severely limit regulation. Milton Lipson, in his book On Guard, has said of this model statute that "It is not an attempt to install basic regulations for the industry but rather one intended to foreclose further criticism."

RAND PROPOSALS	MODEL STATUTE PROVISIONS
Owner, all corporate officers, and all branch managers of contract security agencies (including investigative agencies) should be licensed.	Owner or one corporate officer of contract security companies (not including investigative agencies) should be licensed.
Directors or managers of in-house security forces should be licensed.	No licensing of in-house security forces.
All security employees (including investigators) of in-house and contract agencies should be registered.	Only armed contract and in-house private security officers (not including investigators) should be registered.
Periodic renewal of licenses and registration.	Periodic renewal of licenses and registration.
All licensees and registrants should have high school education or equivalent or pass literacy test.	No education requirement.
Minimum experience requirements for licensing.	Minimum experience requirements for licensing may be waived by passing examination.
Regulatory agencies be given sufficient resources to enable them to screen and monitor licensees and registrants and to investigate violations and impose sanctions plainly explicated in a statute.	Creates Regulatory Board with investigatory and subpoena powers. Does not spell out grounds for revocation or suspension with clarity.

Many states are considering new legislation concerning the regulation of the private security industry. The opportunity to enact an effective regulatory mechanism must not be missed.

The enactment of uniform, rigorous licensing and regulatory statutes across the country would go far toward clearing up the confusion which exists regarding the powers and functions of private police. It would make it simpler to educate the public concerning its dealings with the private law enforcement system. And it would facilitate the development of constitutional standards—the application of the exclusionary rule and Miranda warnings, and creation of standards for search and seizure and interrogation—for the private system of justice./RMH

* * * * * * *

For further reading: (1) The Rand Corporation study, financed by LEAA: J.S. Kakalik and S. Wildhorn, *Private Police in the United States*, 5 vols., R–869/DOJ to R–873/DOJ, U.S. Government Printing Office, $7.85. (2) Milton Lipson, *On Guard: The Business of Private Security*, Quadrangle/The New York Times Book Company, New York, 1975, $10. Among the leading trade journals are *Security World*, and *Security Management* (formerly *Industrial Security*), organ of the American Society for Industrial Security.

[From the Privacy Report, issued by Project on Privacy and Data Collection/ American Civil Liberties Union Foundation, Volume IV, No. 2, September 1976]

Listening In: Governmental Wiretapping and Bugging

Nearly fifty years ago, Supreme Court Justice Louis Brandeis warned that new technological developments permitting eavesdropping on private conversations had "made it possible for the government, by means far more effective than stretching on the rack, to obtain disclosure in court of what is whispered in the closet."

Justice Brandeis' predictions have been realized. The wiretap, the room bug, the miniature radio transmitter, the concealed tape recorder have all made it possible to overhear and preserve what is whispered in the closet, and if these whisperings are not always actually disclosed in a court, the fact that they can be overheard at all has materially affected the privacy of every person.

Electronic eavesdropping is almost as old as the invention of electronic communication. From the middle of the nineteenth century to the present day, every invention for the transmission of communications has been swiftly followed by the development of new methods for intercepting those communications. Among the many uses to which eavesdropping technology has been applied is the gathering of information by government officials for use in criminal and national security investigations.

Not until 1928 did the Supreme Court first confront the question of governmental eavesdropping as a search under the Fourth Amendment. The Court's analysis, delivered in a 5–4 decision in *Olmstead* v. *U.S.*, 277 U.S. 438 (1928), was that the Fourth Amendment prohibited only physical searches, that only material objects, not words, could be "seized," and that electronic eavesdropping accomplished without physical trespass was therefore not a violation of the Fourth Amendment. It was in his dissent to *Olmstead* that Justice Brandeis

sounded the warning about the dangers of governmental eavesdropping, and proclaimed "the right to be let alone" by the government as "the most comprehensive of rights and the right most valued by civilized men." Another dissenter, Justice Holmes, dubbed wiretapping "dirty business," and said he would rather let some criminals go free than have the government "play an ignoble part."

The "dirty business," and the government's "ignoble part" in it, have persisted to the present. In the courts and before the legislatures, government officials have continued to assert that electronic eavesdropping is an essential tool for law enforcement and for the protection of national security. In reply, civil libertarians have argued that such eavesdropping, by its very nature and despite any limitations or controls devised to prevent "abuses," violates Fourth Amendment prohibitions of general warrants and searches, and the constitutional right of privacy.

THE CONSTITUTIONAL QUESTIONS

The authors of the Bill of Rights knew nothing about electronic surveillance technology, but they knew a good deal about general searches. In Colonial America, British officials armed with writs of assistance and general warrants could search private homes at will, without stating what they were looking for or why. The Fourth Amendment was written to make such general searches impossible:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The civil liberties argument proceeds from the assertion that electronic eavesdropping is by definition a general search. When a phone is tapped, every conversation is heard, no matter how irrelevant to the subject of the government's investigation. Moreover, every person using the phone is overheard, and this includes not only every person living or visiting on the premises who may use the phone, but also every person on the other end of the line in every in-coming or outgoing call. Similarly, the room bug picks up every sound uttered by every person who happens to be present in the room. The technology of eavesdropping inherently precludes any "particular description" of what is to be "seized"; once the tap or bug is installed, every word spoken is "seized."

The extent to which the practice of electronic eavesdropping has diminished the right to privacy should be gauged not by the number of conversations which may ultimately be used in a criminal prosecution or described in a government intelligence dossier, but by the kind of inhibitions on freedom of communication that result from the knowledge that no conversation, no matter how innocent or intimate, is immune from intrusion. Thirty-five years after Justices Brandeis and Holmes dissented in *Olmstead*, Justice Brennan predicted that in a society in which eavesdropping devices proliferate, the only way to guard one's privacy will be "to keep one's mouth shut on all occasions." The real danger to the right of privacy, then, arises not so much from the eventual use or disclosure of conversations as from the fact that they are overheard in the first place.

The technology of eavesdropping, at once clandestine and sweeping, is beyond the reach of constitutional controls. But neither the courts nor the legislatures have yet bowed to this fact.

JUDICIAL AND LEGISLATIVE CONTROLS

For many years, judges and legislators have sought to tame the technology of eavesdropping by imposing warrant procedures which appear to satisfy the requirements of the Fourth Amendment.

The Supreme Court rendered a number of decisions dealing with wiretapping and bugging in the four decades after *Olmstead*, but only in 1967 did the Court squarely face the underlying constitutional question. In *Katz* v. *U.S.*, 389 U.S. 347 (1967), involving the installation of a bugging device on the outside of a public telephone booth, the Court interpreted the Fourth Amendment to protect "reasonable expectations of privacy." In this instance, persons using a public phone booth would have such a "reasonable expectation." In *Berger* v. *New York*, 388 U.S. 41 (1967), the Court struck down a New York eavesdropping statute because it did not impose constitutionally sufficient restrictions on the duration and scope of the surveillance. And without such restrictions, said the Court, wiretapping and bugging, even if conducted pursuant to a warrant, would constitute a general search forbidden by the Fourth Amendment.

The *Berger* and *Katz* decisions came at a time of intense legislative debate over the use of electronic eavesdropping in law enforcement. During the '50s and '60s, pressures had been growing in the Congress for federal legislation which would both legitimize and control eavesdropping by government officials, and at the same time restrict the burgeoning private uses of eavesdropping devices. The arguments for a ban on all eavesdropping were made, but passed over in favor of the contention that electronic surveillance is "indispensable" to law enforcement, particularly in the investigation of organized crime. Out of the debate emerged the Federal Wiretap Act, Title III of the Omnibus Crime Control and Safe Streets Act of 1968. 18 U.S.C. § 2510–2520.

Title III purports to overcome the constitutional problems of eavesdropping by incorporating procedures and standards outlined in the *Berger* and *Katz* decisions.

It forbids nonconsentual [1] wiretapping and bugging by federal law enforcement officers except by court order. An order may be issued only for the investigation of specified crimes—a long list of such crimes ranging from treason and kidnapping to gambling and marijuana offenses is provided in the Act—upon a sworn application by the Attorney General or a specially designated Assistant Attorney General which contains a "particular description" of the place where the communication is to be intercepted, of the "type of communication" to be intercepted, and of the identity of the person—if known—whose communications are to be intercepted. The application is supposed to explain why other investigative procedures have failed or cannot be tried, and to state the period of time for which the interception will be re-

[1] Without the prior consent of one party to the communication which is to be overheard. With some restrictions, consentual eavesdropping is permitted by Title III.

quired. The judge must then determine that there is probable cause to believe that the named individual is commiting or is about to commit one of the statutorily enumerated crimes, that particular communications concerning this offense will be obtained by the interception, and that the facilities or premises named will be used by the suspected person. If satisfied on these points, the judge may issue an order limited to a particular person, location, and offense, specifying the particular type of communication which may be sought, and setting a date of termination for the interception—in no case later than thirty days. (Provision is made for extensions by subsequent applications and court orders.)

The Act sets up elaborate record-keeping and reporting procedures, and requires that within ninety days after the termination of a court-ordered interception, the persons named in the order, and such other persons overheard as the judge designates "in the interest of justice," shall be informed of the order and interception—unless the judge, for "good cause," decides to postpone such notice. The Act also imposes certain limitations and conditions on the uses of intercepted conversations as evidence in trials. States are permitted to legislate similar procedures for eavesdropping by state law enforcement officials, so long as their standards are at least as restrictive as those of the federal system.

WHY "CONTROLS" DON'T WORK

On first reading Title III, one might conclude that the constitutional niceties have been honored. To understand why this is not so, it is necessary to examine how electronic eavesdropping under Title III actually works.

During the calendar year 1975, federal and state judges were presented with 704 applications for eavesdropping orders. Of these, only 3 were denied. In 1974, 2 applications out of 730 were denied. Such figures in themselves must cast doubt on the effectiveness of the judicial review provided by Title III. If judges are so compliant as to grant virtually every application placed before them, can any truly meaningful examination be taking place?

The availability of a procedure for "emergency situations," allowing warrantless interceptions for up to 48 hours, only compounds the ineffectuality of Title III's provisions for judicial review. So vague is the statutory definition of the requisite "emergency" that almost any circumstances might qualify. More important, the emergency loophole offers law enforcement agencies a tremendous temptation to conduct warrantless two-day interceptions, or even a series of warrantless two-day interceptions, just to fish for enough solid evidence to support a subsequent warrant application. In fact, such warrantless interceptions might well yield tips leading to other lines of investigation, perhaps even to an arrest, making further eavesdropping by court order unnecessary. (Quite apart from the constitutional questions, the practical necessity for an emergency procedure is doubtful, since it is almost always possible to find a judge to issue a warrant in the time it takes to set up an interception; certainly, it need not take 48 hours.)

It is impossible to say how much warrantless eavesdropping goes on, whether under statutory emergency provisions or altogether out-

side the law. But the evidence suggests, quite a lot. Some of the warrantless surveillances we know of have been connected with narcotics and other criminal investigations, but many have involved the gathering of political intelligence by local police departments, usually forcusing on antiwar and civil rights activists and other such "troublemakers." [2]

The recorded 704 applications for eavesdropping orders in 1975, then, and the 730 in 1974, represent only those interceptions which law enforcement agencies chose to bring to the courts, and probably only those which seemed certain to win judicial approval. The flimsier cases never come into the courts at all.

But even the issuance of a warrant in detailed compliance with Title III requirements does not satisfy Fourth Amendment standards. The law permits the authorization of interceptions lasting up to 30 days, with unlimited numbers of 30-day extensions by court order. The average length of first authorizations for interceptions in 1975 was 22 days; the longest authorization, which included 11 extensions, lasted 360 days. Of 701 eavesdropping authorizations granted, 676 were actually installed (620 wiretaps, the remainder microphone "bugs"), and these yielded an *average* of 654 intercepted conversations apiece, involving an *average* of 71 persons apiece.

The statutory requirements that interceptions be limited both in time and in the type of communication to be "seized" are, for practical purposes, meaningless, because once the eavesdropping device is operating, every conversion is "seized." And that includes even legally privileged conversations, such as those between doctor and patient, husband and wife, and attorney and client—the latter particularly tempting as a source of information about suspected criminal activity. Though prosecutors' reports for 1975 claimed that nearly half of the conversations overheard in court-ordered interceptions contained "incriminating evidence," that still leaves an average of over 300 non-incriminating conversations overheard on each court-ordered installation. One need only reflect on one's own last 300 "innocent" conversations, conducted under a "reasonable expectation of privacy," to understand how intrusive such eavesdropping must be. Consider also how few of the average 71 persons overheard on each court-ordered installation are likely to be connected with the subject of the investigation, much less named in the warrant application. (And recall that those not named in the application will be told that their conversations have been overheard only months later, and even then only at the discretion of a judge.)

Statutory attempts to impose specificity and minimization on searches by eavesdropping, and so to bring them within the Fourth Amendment, are unavailing. It is not just the failure to make Title III or any other legislation sufficiently restrictive. More fundamentally, it is the failure to acknowledge that electronic eavesdropping is inherently an unreasonable search and seizure. The search for an incriminating conversation is not a simple analogy to the search for a blood-stained murder weapon or a cache of stolen jewelry; rather, such a search involves the interception of every spoken word, and the invasion of privacy arises directly from this intrusion, not merely from the eventual use of the evidence in court.

---

[2] Warrantless wiretapping conducted for "national security" and political intelligence purposes by federal agencies is discussed in a later section, below.

Wiretapping and bugging remain in use because the courts and the legislatures have been convinced that they are necessary and productive. Title III was, in fact, enacted in a period of growing public anxiety about organized crime, and largely in response to the insistence of law enforcement spokesmen that electronic eavesdropping is an effective weapon—some claimed the only effective weapon—in the war on organized crime.

Of the 701 eavesdropping orders authorized in 1975, 408 were for suspected gambling offenses, and 178 for suspected narcotics offenses. The next largest categories, loansharking and extortion, and bribery, produced 27 and 21 authorizations respectively. During 1975, 2234 arrests and 336 convictions resulted from the 701 interceptions authorized that year, and 1915 arrests and 2129 convictions resulted from interceptions authorized in earlier years. Such figures may seem substantial, until one poses some specific questions: For what actual crimes were the arrests and convictions obtained? For the most serious offenses specified in the original eavesdropping warrant, or on lesser charges? Was the eavesdropping evidence crucial? Could other means of investigation have proved as fruitful? What were the costs in privacy: how many people were overheard, how many conversations intercepted, what proportion of the people and conversations were actually relevant to the investigation? What were the material costs, in money and personnel?

Professor Herman Schwartz has posed such questions and has analyzed the reported figures for court-ordered eavesdropping from 1968 through 1974 to produce some answers. Schwartz found that from mid-1968 through 1974 a total of 4184 federal and state installations had enabled law enforcement officials to overhear more than 200,000 people engaged in more than 2.7 million conversations. The total cost was almost $22.5 million. By the end of 1974, 6349 convictions had resulted, the great majority for gambling and drug offenses, but the figures do not reveal the severity of the charges on which the convictions were obtained. Schwartz observes that some were only for misdemeanors, and that the absence of reports on sentences imposed obscures the true importance—or lack of it—of the crimes involved.

(Figures presented in the 1976 Report of the National Wiretape Commission tend to bear out Schwartz's suggestion. A survey of sentences for convictions resulting from eavesdropping authorizations for gambling—the category of offenses for which eavesdropping is generally argued to be particularly useful—shows that 58% are limited to fine or probation, and only 22% are longer than one year. For narcotics offenses, the figures are higher: 51% of sentences are longer than one year. But even supporters of electronic surveillance in drug investigations told the Commission they doubted that these convictions had had any significant impact on the volume of narcotics crime.)

The average cost of a 1974 installation was $8087, up from $5632 in 1973, but Schwartz notes that 32 federal installations in the latter year cost $15,000 or more apiece, and 18 of these had not produced even an arrest by the end of 1974. In fact, almost two-thirds of the federal

installations placed in 1971 and 1972 had produced no convictions by the end of 1974.

The Schwartz figures do not prove, nor do they purport to prove, that electronic eavesdropping is useless as a law enforcement technique. No doubt, it can be rather useful to listen in on all the conversations of suspected criminals for days, weeks, even months; sooner or later something interesting could turn up. What the Schwartz analysis does show is the enormous cost, in time and money and especially in privacy, in return for a minimal achievement in fighting crime.

So far, the legislatures and the public have treated the issue of electronic eavesdropping basically as a question of law enforcement. It is viewed as a distasteful but productive method of fighting crime. The assertions of the law enforcement community that eavesdropping is both useful and necessary have been accepted without proof. The fact that the Constitution is part of the trade-off has generally been ignored.

The importance of framing public and legislative debate on wiretapping as a privacy rather than a law enforcement issue was demonstrated recently in Michigan, where the ACLU affiliate organized a coalition of community groups to oppose a package of drug crime bills in the state legislature. The bills were presented, and at first debated, simply as a solution to an alarming rise in the incidence of drug-related crimes in Michigan. But ACLU eventually managed to focus the attention of the legislators and the press on specific provisions for electronic eavesdropping that would authorize "secret entry" to private premises to install and remove eavesdropping devices, require (and pay) landlords and the telephone company to assist such installations, and allow warrantless wiretaps with the consent of one party to the communication—who could be a police informant or undercover agent.

Though the bills did pass the state House of Representatives (they now await action in the Senate), Howard Simon, executive director of the Michigan affiliate, was still pleased: "I really think that our greatest accomplishment can be seen in the fact that the debate in the public press and on the floor of the House of Representatives was framed in terms of the issues set by the American Civil Liberties Union."

EAVESDROPPING FOR INTELLIGENCE

Supporters and opponents of eavesdropping alike recognize that the technique is more effective as a means of gathering intelligence than as a method for solving crimes. "As a rule," the Report of the National Wiretap Commission observes, "court-ordered electronic surveillance has proven useful in the investigation of offenses which are being or are about to be committed. Where the offense has already been completed, surveillance is rarely used." One of the principal arguments for using eavesdropping to combat organized crime is that here the investigation is directed against "known criminals but unknown crimes." Eavesdropping purportedly allows investigators to penetrate the secret, tightly knit hierarchies of syndicate crime, and to gather "strategic intelligence"—numerous small pieces of incriminating evidence that might eventually add up to bring a conviction. Of

course, to gather such intelligence usually requires extensive eavesdropping, involving many people, many conversations, and many weeks, months, or even years. It requires, in fact, precisely that unrestricted use of electronic surveillance which was forbidden by *Katz* and *Berger* and, supposedly, by Title III as well. Strategic intelligence does not focus on a specific crime or a single suspect; its object cannot be "particularly described." Rather, as the testimony of many experienced investigators has clearly revealed, the search for strategic intelligence necessitates the surveillance of all of the subject's activities, not merely those which are legally suspect, and embraces all his family, friends, associates, and acquaintances. Thus, where eavesdropping is supposedly most useful, it is also most abusive.

If eavesdropping is regarded as an effective means of gathering criminal intelligence, it is thought to be invaluable as a means of gathering political intelligence. Wiretapping and bugging have long been staples of the political surveillance operations conducted by dozens of federal agencies and by local police departments all over the country. The targets have almost always been the practitioners of some variety of political dissent. Eavesdropping for political intelligence reaches directly into areas protected from governmental inquiry or interference by the First Amendment. And because most political eavesdropping is conducted without warrants, there is no judicial oversight to minimize incursions on Fourth Amendment rights. The gathering of political intelligence through electronic eavesdropping is the ultimate realization of Justice Brandeis' predictions half a century ago.

There is no statute which specifically authorizes eavesdropping for purposes of political intelligence. Title III limits eavesdropping by court order to investigations of criminal acts and conspiracies. But it also states, § 2511(3), that nothing in the statute "shall limit the constitutional power of the President to take such measures as he deems necessary" to protect the national security. Congress did not define the nature of that purported constitutional power, but the intelligence community has apparently interpreted this "saving clause" to sanction electronic surveillance of just about anyone without court order or judicial oversight, under the President's supposed "inherent power" to protect the national security.

Recently, the courts have whittled away at that claim, notably in *U.S.* v. *U.S. District Court*, 403 U.S. 297 (1972) (commonly called the *Keith* decision), in which the Supreme Court ruled that warrantless wiretaps could not be used in domestic security investigations, not involving foreign agents or foreign powers, under the authority of the President's "inherent powers." The Court held that the President's powers are limited by the Bill of Rights, and rejected the argument that matters of national security are beyond the reach of judicial competence. Three years later, the Court of Appeals for the District of Columbia declared that even where the subjects of a security investigation are engaged in activities which affect foreign affairs, warrantless wiretaps may not be used against a domestic organization if it is not "the agent of nor acting in collaboration with" a foreign power. *Zweibon* v. *Mitchell*, 516 F. 2d 594 (D.C. Cir., 1975). And in 1976 the U.S. District Court for the District of Columbia ruled that warrants are required even when the subjects of investigation are living over-

seas, if they are not agents of a foreign power. *Berlin Democratic Club* v. *Rumsfeld*, Civil Action No. 310–74 (March 17, 1976).

The American Civil Liberties Union has always maintained that the President possesses no inherent power to circumvent the law and the Bill of Rights under any circumstances. The Church Committee—the Senate Select Committee on Intelligence, which conducted a fifteen-month study of the government's domestic spying activities—apparently agreed, for its first recommendation stated flatly, "There is no inherent authority for the President or any intelligence agency to violate the law."

Now civil libertarians are engaged in still another attempt to focus public attention on the constitutional issues raised by electronic eavesdropping. This time the context is a proposal to "reform" eavesdropping for intelligence-gathering purposes by legitimizing it. S. 3197, the Foreign Intelligence Surveillance Act, would authorize electronic surveillance of Americans engaged in "clandestine intelligence activities" (of undefined nature) and would, for the first time, give legislative definition and recognition to the President's purportedly inherent "constitutional power . . . to acquire foreign intelligence information." In the guise of reform—centering primarily on an exceedingly ineffectual warrant procedure to be required for intelligence eavesdropping—S. 3197 would in fact lend Congress' blessing to the very abuses it is supposedly set upon correcting, and give legislative approval to the dangerous proposition that the President is above the Constitution.

* * * * * * *

Because of Watergate and the revelations, which seem to come almost daily, of the abusive practices of the intelligence agencies over the last several decades, attention is focused for the present on the issue of wiretapping in the context of national security. Yet the present crisis is not an isolated problem. Rather, it only illustrates in particularly vivid form the truth of the position that ACLU has been espousing for years: that all wiretapping is abusive, and that governmental eavesdropping under any circumstances is inherently a violation of the constitutional right to privacy./TRH

[From the Washington Star, Dec. 9, 1976]

U.S. Probes Sale of Confidential Medical Records

(By John J. Fialka)

Investigators from the FBI and the Internal Revenue Service are probing the operations of a Chicago investigative service that appears to have built a flourishing business by gaining unauthorized access to medical records and selling the information to many of the nation's largest insurance companies.

One of the reasons the investigators are so interested is that there are indications that the firm—called Factual Service Bureau, Inc.—may have sold copies of confidential records from a variety of federal agencies, including the FBI and the IRS.

So far, there is evidence that at least 55 firms—including many of the nation's most prestigious insurance companies—did business with Factual, which, until recently, had offices in 15 cities across the country.

In many cases, according to subpoenaed company documents, Factual advertised its skills openly.

A form letter that was sent by the firm to insurance company claims officers states: "Our investigation reports cover all medical aspects of a claim, whether you have authorization or not." Documents indicate that Factual was able to obtain even the most sensitive types of hospital information without authorization, including individual psychiatric records and, in one case, detailed clinical observations of a retarded child.

Reports made by company investigators repeatedly boast of "sources" that provided them with criminal records from the FBI's computerized Crime Information Center (NCIC).

One report to an insurance company refers to "confidential sources" within IRS's Kansas City office who provided them with various numbers and detailed information from the tax returns of an 84-year-old Chicago woman being investigated, including an itemized list of her investments.

Others refer to sources within Veterans' Administration and Social Security offices who provided them with individual claims for disability benefits.

Asked about the matter, spokesmen for both Social Security and the Veterans' Administration said they had no indication that agency files had been penetrated by Factual.

The man who first unearthed evidence of Factual's widespread dealings is Dale Tooley, Colorado's district attorney for Denver, who said he was approached by a lawyer and a private investigator last fall. They complained that Factual was building its business reputation by use of improper methods.

"At that point my secretary was in the hospital and we decided to see if they could get her records," explained Toolely, who retained the services of Factual through the two men. "They came back with records from two hospitals. They weren't just Xeroxed copies either, they were the originals."

After that revelation, Tooley's office swooped down on Factual's Denver office in October 1975 and seized over 1,000 case folders, training manuals and other documents, a pile of evidence that, according to Tooley, "is really the tip of a nationwide iceberg."

So far, Tooley has obtained indictments against 20 defendants, including three insurance companies: Northwestern National Insurance Co., of Milwaukee, Wis.; Home Insurance Co., of New York, and Reliance Insurance Co., of Philadelphia.

Those indicted include two top officers of Factual, William J. Severin, Jay G. Barker, and the company's public relations man, William Kizorek. They are charged with conspiring to promote theft, criminal impersonation and embezzlement of public property.

Since most of Factual's activities went far beyond the state of Colorado's legal reach, Tooley obtained grand jury authorization to share some of his evidence with federal law enforcement agencies and the U.S. Privacy Protection Study Commission, which is working on ways to strengthen individual privacy rights.

According to those familiar with the case, Factual is suspected of having sources in at least two police departments. The sources would check out names for them with the FBI, using NCIC computer terminals. An FBI spokesman confirmed that this matter is being investigated. The allegation, he said, is a rare one. "We've never had any instance of what you would call an illegal penetration of the computer."

One of the sources was reportedly a man somewhere in the New York Metropolitan Police Department who answered a special phone with the code phrase. "This is Officer O'Mally with the 101st Precinct." O'Mally, or whoever he was, allegedly would take names from Factual agents and check them out on the department's NCIC terminal.

A press spokesman for the police department said that he thought the procedure sounded "impossible." Asked if the department was investigating, he said, "If we were, I couldn't tell you."

Factual's reports to insurance companies indicate the company also had a wide variety of "sources in other agencies." One report says Factual "had our sources check the claimant's Army record" at the Department of Defense's Bureau of Permanent Records in St. Louis, Mo., to see if the person had been discharged on a "Section 8," or a ruling of mental incompetence.

Another refers to a "confidential source" at the Veterans Administration. And another refers to "confidential sources" who searched through personnel files in the federal office building in Denver and found an employe's disability retirement papers.

When sources were not available, evidence shows that Factual used a subterfuge that company employes called "pretexting." It amounted to impersonating police officers, welfare officials, IRS agents and doctors on the telephone. The most common ruse was impersonating a doctor because obtaining unauthorized medical information was Factual's "bread and butter" business, according to company records.

According to a Factual training manual, obtained by Tooley's office in Denver, investigators were given the following instructions on how to do it:

"1. Don't use a doctor's name who is known in the area.

"2. Write down the name of the doctor you are using to avoid forgetting it.

"3. Have a referral phone number in case they want to call you back. This could be the number of another hospital.

"4. Then call that (the other) hospital and advise them you are expecting a call and will call the party back."

Tooley's evidence includes a picture of one Factual investigator using another "pretext." He was dressed as a Roman Catholic priest, a costume he allegedly used when looking for medical information in certain hospitals and in Spanish-speaking neighborhoods.

Factual's case already has attracted some interest on Capitol Hill. Rep. Barry Goldwater Jr., R–Calif., a member of the Privacy Commission, found there was one case involving one of his constituents, a youth who was being treated in two special Los Angeles facilities for mental retardation sustained as the result an allegedly improper prescription of a drug, which was the subject of a malpractice suit. Factual had obtained detailed records and observation reports on the youth from both institutions without obtaining consent from his parents, according to Goldwater.

"It's the most unbelievable thing I've ever seen," said Goldwater. "There has got to be some special concern here."

Goldwater has introduced legislation that would allow a citizen to sue a hospital or the government if confidential records are released.

The financial conduits that gave Factual a business that came to as much as $4 million a year, according to some estimates, begin with the client insurance company, which receives an injury claim.

The states regulate the insurance industry and, under most state laws, when a claim is submitted a company is immediately required to put an amount of money that would satisfy the claim in an escrow account, a practice called "reserving" the claim, while the claim is analyzed.

Rather than go to court, where they could legally obtain access to the plaintiff's medical files through a process called discovery, many insurance claims officials apparently chose a much quicker route—hiring Factual—so the claim could be settled and what remained of the reserved funds could be put back into an interest-bearing account.

According to testimony by Factual's Denver employes, the company regarded itself as the "Cadillac" of the investigative industry. Its employes were paid about three times the average salaries paid by insurance companies. Its charges were often in the upper range of fees charged by investigators.

Just what has happened to Factual since Tooley began his investigation is not clear. If you call their Chicago headquarters number, a woman will answer "Inner Facts, may I help you?"

The president of Inner Facts is W. J. McIntyre, who, when questioned by a reporter, admitted that he is a former employee of Factual. He insisted, however, that there is "absolutely no connection" between Inner Facts and Factual other than the use of the same phone number and residence in the same downtown Chicago office building.

"Factual went out of business in January. It became defunct approximately in the first month of 1976," said McIntyre.

Reached at his home in suburban Chicago, Kizorek said he could not comment "under instructions from my attorney." The person who answered Severin's phone in Wilmette, Ill., refused to respond to any questions. "Send us a letter," he said. Barker could not be reached for comment.

During the past year, as news of Factual's problem in Denver began to filter through the insurance industry, some companies moved quickly to sever their ties with the investigatory service. For example, there was considerable consternation at Aetna Life & Casualty, the nation's fourth largest casualty underwriter, when company executives found it had had dealings with Factual. Aetna's president, William O. Bailey, is a member of the Privacy Commission.

According to S. Benton Guiney, Jr., the company's vice president in charge of claims, after Bailey found out what Tooley had unearthed in Denver, he issued a "broadside" ordering company claims officials not to use Factual "or any similar service."

"I regard this incident as a scandalous thing," said Guiney. After interrogating local office managers as to "how we got into this," Guiney said that "some of the answers seem naive, but I have to guess they didn't know what methods they (Factual) were using." He said Aetna found "only four or five" local offices that were using Factual.

A spokesman for State Farm, the colossus of the auto insurance industry, said that the company's field force was ordered to stop "all relationships" with Factual in January. Since then, he said, company attorneys have been able to turn up only one case where medical records were obtained without authorization.

A spokesman for Mutual of New York said that his company has canceled dealings with Factual after using them "on four occasions in the last 10 years."

A spokesperson for Allstate Insurance Companies admitted that the firm had used Factual's services once or twice a year on a "very limited basis." Relations with the company, she said, were terminated a couple of months ago "because of their reputation."

A spokesman for Travelers Insurance Companies said that it used Factual about a dozen times in the last four or five years. "As soon as we found out there were some allegations of misconduct, we terminated their services," the spokesman said.

A representative of Kemper Insurance Co. in Chicago said that the company has used Factual's services throughout the country "maybe 50 times in the last five or six years," and has no policy against using Factual in areas other than Denver.

A spokesman for the Hartford Insurance Group said that Factual was one of the company's "lesser used" investigative agencies in the past. Factual, he said, is no longer used "as the result of the exposure of their operating methods."

Charles H. Foelber, senior executive vice president for U.S. Fidelity & Guaranty Co., said he would make "no comment" whether his company has had any dealings with Factual. Factual once sent out a form letter calling the $1.8 billion company "our No. 1 client in the entire country."

A spokesman for Prudential said that the company had no records that show any dealings with Factual. Sources familiar with the evidence from Factual's Denver office, however, indicated that Prudential's name appears on Factual's client records.

Tooley says he wonders about the insurance companies' explanations that they were not aware what Factual was doing. He recently told the Privacy Commission that he found copies of "hundreds of letters" in Factual's Denver office soliciting business from various insurance companies.

"Not only did hundreds of insurance companies receive those solicitations, that the investigators could secure medical records without authorization, but we found no instance in which the insurance companies reported that solicitation to the authorities," the prosecutor said.

"The evidence we have," he added, "is they full well know how the records were sought. They are experts after all in this business of knowing what can and cannot be gotten through court and authorization procedures."

[From the Federal Times, Dec. 13, 1976]

Microwave Weapons Study by Soviets Cited

The Defense Intelligence Agency has released a report on heavy Communist research on microwaves, including their use as weapons. Microwaves are used in radar, television and microwave ovens. They can cause disorientation and possibly heart attacks in humans.

Another biological effect with possible anti-personnel uses is "microwave hearing."

"Sounds and possibly even words which appear to be originating intracranially (within the head) can be induced by signal modulation at very low average power densities," the report said.

According to the study, Communist work in this area "has great potential for development into a system for disorienting or disrupting the behavior patterns of military or diplomatic personnel."

No mention was made of the still-unexplained microwave bombardment of the American Embassy in Moscow.

The study dealt largely with long-term exposure of days or weeks in industrial situations, which usually produce mild effects. Short exposure to intense radiation can cause heart seizure and a wide range of physical disorders.

○