Subject: Introduction

To: All Supervisors and All Manual Holders of the Interception and Recording of Wire, Oral and Electronic Communications Manual

Filing Instructions:

- Remove and destroy pages 7 and 8 of Chapter 1, dated 03/01/2006, and replace with the attached revised pages.
- File this Policy Memorandum in front of this section.
- These materials are to be reproduced locally for all holders of the Interception and Recording of Wire, Oral and Electronic Communications Manual.
- This directive is in effect until superseded.

Impact Statement: This directive restores previously deleted material under the heading of "Security of Non-Telephone Consensual and Non-Consensual Intercept Equipment" with regards to the ledger book.

Mandatory Review: The Responsible Office will review all policy contained in this section in its entirety by or before March 2009.

Questions regarding this policy should be directed to the Investigative Support Division at 202-406-5773.

Brian K. Nagel
AD - Investigations

DCP#: WIM 2006-3

RIF

Introduction
Table of Contents

INTRODUCTION

The purpose of this manual is to outline the legal and administrative procedures which must be followed when conducting either consensual or non-consensual interceptions of wire, oral, or electronic communications; or when utilizing pen registers, vehicle locator systems (VLS), telephone traps and traces; or when requesting governmental access to stored electronic communications.

In addition to the Fourth Amendment of the Constitution, there are a number of statutes and executive orders which govern the conduct of interceptions of wire, oral or electronic communications, both consensual and non-consensual.

The procedures used to conduct these interceptions are based upon procedures established by the Criminal Division of the Department of Justice pursuant to Title 18, United States Code, Sections 2510 to 2522; Title 18 Sections 2701 to 2712; Title 18 Sections 3121 to 3127 (Title I, II and III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986 (ECPA); the Communications Assistance for Law Enforcement Act of 1994 (CALEA), the Antiterrorism and Effective Death Penalty Act of 1996 (Antiterrorism Act)), the USA-Patriot Act of 2001, and The Homeland Security Act of 2002.

Although this Service may conduct interceptions pursuant to any of the aforementioned laws and regulations, the overwhelming majority of interceptions are conducted pursuant to the provisions of Title I, II, and III of the Electronic Communications Privacy Act of 1986. Since the other statutes are so diverse and so infrequently used by this Service, they are not addressed in this manual.

All requests for authorization of communication interceptions which are subject to provisions of statutes other than those incorporated in the Electronic Communications Privacy Act of 1986, should be directed to the Intelligence Division. The Intelligence Division, in conjunciton with the Investigative Support Division, will coordinate the conduct of the interception and ensure all statistical and record keeping functions are accomplished.

All of the guidelines contained in this manual have been designed to assure strict adherence to the laws and rules that govern the use of these types of interceptions. It is the philosophy of the Secret Service that it is preferable to err on the side of caution rather than risk any inadvertent violation of law or established procedure when conducting such interceptions.

Overview of the Electronic Communications Privacy Act of 1986 (Public Law No. 99-508)

This act is divided into three separate, but closely related titles: Title I - Interception of Communications and Related Matters; Title II - Stored Wire and Electronic Communications and Transactional Records Access; and Title III - Pen Registers and Trap and Trace Devices. The policies and procedures incorporated under this act became effective on January 20, 1987.

Since the act includes provisions for both civil and criminal penalties, all offices contemplating the use of investigative techniques covered under the act are cautioned to consult with the appropriate Office of the United States Attorney prior to implementation.

Definitions and Explanations

Department of Justice: For the purpose of this manual, Department of Justice refers to the Office of Enforcement Operations, DOJ, Washington, D. C.

Wire Communications: The definition of "wire communication" means any "aural transfers" made in whole or in part through the use of facilities for the transmission of communication by the aid of wire, cable or other like connection between the point of origin and the point of reception as defined in 18 U.S.C. 2510 (1). Wire communications are specifically excluded from the definition of electronic communications, 18 U.S.C. 2510 (12) (A).

Oral Communication: 18 U.S.C. 2510 (2) defines oral communication as any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interceptions under circumstances justifying such expectation.

Oral communication, as defined, is specifically excluded from the definition of electronic communication.

Intercept: 18 U.S.C. 2510 (4) defines intercept as the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.

The "or other" was added to accommodate the non-aural acquisition of electronic communications.

Electronic Communication: 18 U.S.C. 2510 (12) defines "electronic communication" as any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or part by a wire, electromagnetic, photo electronic, or photo-optical system that affects interstate or foreign commerce.

"Electronic communication" is also specifically defined to exclude a wire or oral communication. The effect of the breadth of this definition is that any and all forms of electronic communications, unless specifically exempted, are now subject to statutory provision, just as wire and oral communications have been since 1968.

Electronic, Mechanical or Other Device: 18 U.S.C. 2510 (5) defines electronic, mechanical or other device as any device or apparatus which can be used to intercept 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; 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.

Video Surveillance

Video surveillance or use of closed circuit television (CCTV) is not regulated by Title I, but it is frequently part of an application for electronic surveillance. When there is a reasonable expectation of privacy in the place to be videotaped, prior approval from an appropriate DOJ official and a court order is required before such video surveillance may be used in an investigation. A court order and prior DOJ approval is required unless the surveillance is used to record events in public places or places where the public has unrestricted access, and where the camera equipment can be installed in places to which investigators have lawful access.

If a court order is required, the pleadings are to be based on Rule 41 of the Federal Rules of Criminal Procedure and the All writs Act (28 U.S.C. Section 1651).

Exceptions

Because the definition of electronic communication is so broad and all-inclusive, it became necessary to provide exceptions. The exceptions dealt with forms of electronic communications that either appeared patently not to be deserving of privacy protection or where a policy decision was made by the Congress not to include a specific form of electronic communication.

These exceptions appear in the legislation either as exceptions as defined in 18 U.S.C. 2510 or as exceptions to the section that penalizes certain activity as unlawful, 18 U.S.C. 2511. These exceptions are as follows:

1. **Tone only paging devices.** It has been the position of the Department of Justice that intercepting tone beeps or vibrations from a pager is not a search and, therefore, such interceptions raise no Fourth Amendment implications; the current statute endorses this policy. By contrast, digital display and voice paging devices are covered by the current statute (see Chapter IV of this manual).

2. **Communications from tracking devices (beepers) placed in automobiles or packages to trace their location. 18 U.S.C. 2510 (12) (C).** These are specifically excluded from this legislation because of the manner in which they function and the limited privacy implications related to their use. This area is being left to case law development.

3. **Pen registers, and trap and trace devices.** These investigative tools qualify as electronic communications as that term is broadly defined. Since the privacy interests involved are so limited with these techniques, they have been excluded from the coverage of Title I of the current statute.

4. 18 U.S.C. 2511 (2) (h) (i). However, Title III (Chapter 206, 18 U.S.C. 3121-3127, of the Federal Criminal Law Handbook) of the statute specifically regulates these techniques. By and large this Title, to be discussed in Chapter IV of this manual, merely codifies existing Department of Justice policy and practices on pen registers/trap and trace devices.

5. **Certain radio communications.** The definition of electronic communication is so broad that it sweeps in all forms of radio communications. Thus, it was necessary for the statute to specifically exclude various forms of radio communications that patently should not be subject to protection from interception such as electronic communications that are broadcast so as to be readily available to the public (AM and FM radio station broadcasts), ship to shore general public type communications, citizen band radio, general mobile radio services and the like. Reference is made to 18 U.S.C. 2511 (2) (g).

This subsection of the statute also contains other specific exceptions relating to interaction with the Federal Communications Act or where there is a necessity to service the system or locate interference. A review of Chapter 119 of the Federal Criminal Code and Rules is strongly recommended.

Reference is made to pertinent sections relating to the conduct of electronic surveillance to be found in the U.S. Attorney's Manual, Title 9, Chapter 7.

Title I - Interception of Communications and Related Matters

The 1986 statute defines and regulates three types of communications: (1) wire; (2) oral; and (3) electronic communications. The last type, in essence, is any form of communication using electronics in which the human voice is not utilized.

It should be noted that the act mandates little change in the substantive or procedural requirements for obtaining an order to intercept a traditional wire or oral communication. In explaining the provisions of the act and the provisions set forth in the administrative guidelines which apply to interceptions not specifically provided for in the act (primarily Titles I and III), Title I of the current act largely replaces Title III under the old statute. Additional crimes have been added to the list of crimes enumerated in 18 U.S.C., Section 2516 for which a wire or oral interception order can be obtained. These additional crimes include the following, which may impact directly on this Service's operations:

18 U.S.C. 1203 (hostage taking);

18 U.S.C. 1029 (fraud and related activity in connection with access devices);

18 U.S.C. 115 (threatening or retaliating against a federal official) and;

18 U.S.C. 2511, 2512 (interception and disclosure of certain communications and use of certain interception devices).

In addition, a subsection (18 U.S.C. 2516 (1) (l)) was added that authorizes interception to ascertain the location of any fugitive from justice from an offense described in 18 U.S.C. 2516 (1). Section 2518 of Title 18, which describes the procedure for intercepting wire, oral, and now electronic communications, remains substantially the same under this law.

Title II - Stored Wire and Electronic Communications and Transactional Records Access

Title II of the act is designed to protect the privacy of stored electronic communications, either before such a communication is transmitted to the recipient or, if a copy of the message is kept, after it is delivered.

In developing the legislation, electronic communications were divided into two categories: (a) communications during the transmission stage, and (b) communications in "storage."

Electronic Storage is defined in 18 U.S.C. 2510 (17) as both any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and the storage of such communication by an electronic communication service for purposes of backup protection of such communication. There was general recognition that the interception of communications during the transmission stage is more intrusive than of those in storage, and accordingly, those communications were given almost the same protection as that provided for wire and oral communications.

Stored communications were likened to regular mail being handled by the Post Office. Under present day standards, a search warrant would be required to intercept mail since it enjoys Fourth Amendment protection. Congress ultimately decided that electronic mail in storage incident to transmission should be accorded the

same protection. The same principle applies to "backup" copies made by the providers of electronic communications services.

Therefore, Fourth Amendment type protection will be accorded to the stored data for the first 180 days, requiring a search warrant under Rule 41 of the Federal Rules of Criminal Procedure for government access. After the 180 day period expires, any records still retained would revert to the status of third party records and would be available by administrative or grand jury subpoena, a court order, or warrant. The most important provisions of Title II are the following:

Unlawful Access to Stored Communications

18 U.S.C. 2701 makes it an offense to (a) intentionally access, without authorization, a facility through which an electronic communication service is provided; or (b) intentionally exceed the authorization of such facility; and as a result of this conduct, obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such a system.

This provision is intended to address the increasing problem of both unauthorized "computer hackers" and corporate spies who deliberately gain access to, and sometimes tamper with, electronic communications that are not available to the public. The provision is not intended to criminalize access to "electronic bulletin boards," which are generally open to the public so that interested persons may communicate on specific topics.

In addition, a communication will be found to be readily accessible to the general public if the telephone number of the system and other means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy.

Disclosure of the Contents of a Stored Communication

18 U.S.C. 2702 (a) generally prohibits the provider of a wire or electronic communication service from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient of the communication. The originator, addressee, or intended recipient can give lawful consent to divulge the content of the communication.

18 U.S.C. 2702 (b) provides eight distinct exceptions that modify the general prohibitions against disclosure contained in 2702 (a). (See Chapter 5 for further explanation.) The eight exceptions allow disclosures to a law enforcement agency, if the contents were:

(a) Inadvertently obtained by the service provider; and

(b) Appear to pertain to the commission of a crime.

Similarly, 18 U.S.C. 2511 (3), as amended, prohibits such a provider from divulging the contents of a communication while it is in the transmission stage.

Requirements for Governmental Access to Stored Communications

18 U.S.C. 2703 provides that a governmental entity may only obtain access to the contents of an electronic communication that has been in storage for 180 days or less pursuant to a search warrant. If the message has been stored for more than 180 days, the government can obtain the information by a variety of procedures including a search warrant, grand jury subpoena, administrative subpoena, or a court order, depending on the type of notification the government wishes to provide.

18 U.S.C. 2703 (b) relates specifically to records held in remote computing systems and such records that are not mentioned anywhere in 18 U.S.C. 2703 (a).

Procedures for Access to Transactional Information Including Telephone Records

18 U.S.C. 2703 (c) sets forth the rules under which the government may obtain access to transactional records with or without the consent of the subscriber. These are records that pertain to the subscriber to, or customer of, an electronic communication service or remote computing service and which do not involve the contents of a communication. It should be noted that transactional records include toll records. The government will be able to obtain such transactional records by grand jury subpoena, administrative subpoena, search warrant, or court order based upon a finding of relevancy.

Backup Preservation of Information in Storage

18 U.S.C. 2704 sets forth the procedures that apply to backup copy preservation. This is the provision that will permit law enforcement officials to have a copy made, in the nature of a picture of the records that exist on a given day, of records of illegal activities in which a computer storage or remote processing firm is utilized in the criminal activity.

Delayed Notice

18 U.S.C. 2705 describes the circumstances under which the government may delay notification to the customer or subscriber.

Title III - Pen Register and Trap and Trace Devices

Chapter 206 (18 U.S.C. Section 3121 to Section 3127) of the Federal Criminal Law Handbook covers Title III of the Electronic Communications Privacy Act of 1986. The Title begins with a general prohibition against the use of a pen register or a trap and trace device without first obtaining a court order pursuant to 18 U.S.C.

3123 or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.). This chapter, in essence, codifies the existing Department of Justice policy of obtaining a court order to authorize the installation of a pen register or a trap and trace device, and sets forth the procedure for seeking such an order.

> NOTE: Under the provisions of the USA PATRIOT Act of 2001, the analysis remains unchanged with respect to the Fourth Amendment and the wiretap statute. However, substantial amendments to the definition of "Pen Register" and "Trap and Trace Device" alter the applicability of the pen/trap statute.

Title I, II and III (General)

A review of Chapters 119, 121, and 206 of the Federal Criminal Law Handbook is strongly recommended. Further reference is made to pertinent sections relating to the conduct of electronic surveillance to be found in the U.S. Attorney's Manual, Title 9, Chapter 7.

Communications Assistance for Law Enforcement Act (CALEA)

In October 1994, at the request of the nation's law enforcement community, Congress enacted the Communications Assistance for Law Enforcement Act, or CALEA. The CALEA clarified the scope of a telecommunications carrier's duty in effecting lawfully-authorized electronic surveillance and addressed previous deficiencies in the Electronic Communications Privacy Act. The CALEA requires telecommunications carriers to modify the design of their equipment, facilities, and services to ensure that lawfully-authorized electronic surveillance can actually be performed.

Security of Non-Telephone Consensual and Non-Consensual Intercept Equipment

Due to the sensitivity of this type of equipment, it must be centrally located in one safe within each office or in a properly secured vault room within the office. In most cases, non-consensual equipment will be maintained within the Technical Security Division (TSD).

General access to the equipment should be limited to a minimum number of individuals, preferably supervisors, either by the squad supervisor, or in offices where assigned, the Physical Security Specialist, who are assigned to maintain, check out, check in, and secure the equipment. The record-keeping system controlling the use of the equipment must utilize a bound ledger book for this purpose.

The ledge book should be prepared with columns reflecting the following fields of information:

1. Date out - date that equipment is taken from storage.
2. Case Number - self-explanatory.

3. Equipment - description of item.
4. Serial and/or SS property number - self-explanatory.
5. Assigned to - last name of SA to whom equipment is being issued.
6. SA initials - Initials of SA to whom equipment is being issued.
7. Check out by - Initials of supervisor or other designee.
8. Date in - date item returned to storage.
9. Check in by - Initials of supervisor or other designee.

Reports to the Department of Justice

Non Consensual

The provisions of title 18 U.S.C. 2519 mandate that the Secret Service submit an annual report, due in January, to the Attorney General or the Assistant Attorney General of the United States regarding non-consensual intercepts. This report will cover each application for any non-consensual wire, oral, or electronic interception order made by this Service under provisions of the Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic Communications Privacy Act of 1986.

Consensual

There are no reporting requirements to the Attorney General for consensual monitoring. However, DOJ requires an agency to maintain the records of all consensual monitoring. Investigative Support Division (ISD) will maintain all the consensual monitors approved and conducted for three (3) years per General Records Schedule 23.