# PRIVACY, COMPUTERS AND THE PATRIOT ACT: THE FOURTH AMENDMENT ISN'T DEAD, BUT NO ONE WILL INSURE IT

*Steven A. Osher*[*]



> "Grave threats to liberty often come in times of urgency, when constitutional rights seem too extravagant to endure."[1]
>
> —Justice Thurgood Marshall, 1989

## I. INTRODUCTION

The tragic events of September 11, 2001 shocked the nation with their incomprehensible devastation and the stunning message of America's domestic vulnerability. At no time in recent memory, if ever, had Americans felt so threatened on their own soil. Because this was not the act of any identifiable geographic state, America was initially powerless to retaliate using its unparalleled military forces. Clearly, however, urgent measures were needed to restore domestic security. Congress quickly responded with the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, commonly known as the USA PATRIOT Act (USAPA).[2]

This Essay examines the USAPA, in particular its effects on cyber communications and Fourth Amendment[3] guarantees against unreasonable

---

* For Sam.

1. Skinner v. Ry. Labor Executives Ass'n, 489 U.S. 602, 635 (1989) (Marshall, J., dissenting).

2. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter USAPA].

3. U.S. CONST. amend. IV reads:

> 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.

searches and seizures. Part II examines the provisions of the USAPA that most directly affect computer privacy. Part III discusses the history of crisis-driven legislation designed to enhance national security by trimming civil liberties. The final section evaluates the legislation, its effects, and appropriateness.

Representative F. James Sensenbrenner, Jr. introduced the bill in the House in response to the September 11th hijackings and subsequent attacks on the World Trade Center Towers and the Pentagon.[4] The USAPA broadens the authority of the intelligence-gathering and criminal investigative branches of government in the areas of electronic taps and traces, immigration, and border patrols.[5] Citing the urgent need for new "tools" to fight terrorism,[6] Attorney General John Ashcroft exhorted Congress to pass the 243-page bill within a week.[7]

After the House Judiciary Committee amended the bill to better comport with constitutional guarantees,[8] House Speaker Dennis Hastert and other Republican leaders scuttled it in favor of a new bill,[9] in a process described as "one of the most undemocratic breakdowns in the history of our legislative process."[10]

Under pressure to react to the events of September 11th, and operating from temporary offices as a result of the threat of anthrax contamination,[11] Congress passed the measure with "few hearings and little debate."[12] The vote was 357 to 66 in the House.[13] Representative John Conyers complained that only two copies of the bill were made available to the Democrats before the vote, providing little opportunity for lawmakers to

---

*Id.*

4. *See* Allison L. de Cerreño, *Section 208 of the PATRIOT Act Walking a Fine Line Between Security and Free Exchange of Scientists and Knowledge, available at* http://members.nyas.org/events/policy/pol_01_1023.html (last modified Oct. 26, 2001).

5. *Id.*

6. *See* Jim McGee, *An Intelligence Giant in the Making; Anti-Terrorism Law Likely to Bring Domestic Apparatus of Unprecedented Scope*, WASH. POST, Nov. 4, 2001, at A4.

7. Nat Hentoff, *Why Should We Care? It's Only the Constitution: Terrorizing the Bill of Rights*, THE VILLAGE VOICE ¶ 3 (Nov. 9, 2001), *at* http://www.villagevoice.com/issues/0146/hentoff.php.

8. *Id.* ¶ 4.

9. *Id.* ¶ 9.

10. *Id.* ¶ 3.

11. *See* Robert Scheer, *With Powers Like These, Can Repression Be Far Behind?,* L.A. TIMES, ¶¶ 1, 7 (Oct. 30, 2001), *at* http://www.latimes.com/news/opinion/la-oe-sheer30oct30.story.

12. Laura Donohue & Jim Walsh, *Patriot Act—A Remedy for an Unidentified Problem,* SAN FRANCISCO CHRON. (Oct. 30, 2001), at A17, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2001/10/30/ED10681.DTL.

13. Stefanie Olsen, *Patriot Act Draws Privacy Concerns,* CNET NEWS.COM: TECH NEWS FIRST ¶ 3 (Oct. 26, 2001), *at* http://news.cnet.com/news/0-1005-200-7671240.html.

comprehend its implications.[14] Representative Barney Frank, one of the drafters of the Judiciary Committee changes that were removed from the final draft, characterized the vote as "the least democratic process for debating questions fundamental to democracy I have ever seen. A bill drafted by a handful of people in secret, subject to no committee process, comes before us immune from amendment."[15] "Why should we care?" remarked Representative David Obey, "It's only the Constitution."[16]

The Senate passed the bill by an overwhelming 96-1 vote.[17] Senator Russell Feingold, the lone dissenter in the Senate, remarked that "few in Congress had even read summaries, let alone the fine print, of the document they so hastily passed."[18] Apparently, dissent was stifled by the reluctance of lawmakers to appear "soft on terrorism."[19]

## II. USAPA PROVISIONS

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. 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?[20]
>
> –Justice Louis Brandeis, 1928.

The chief areas examined in this Essay concern the expansion of surveillance powers in wiretaps, search warrants, and subpoenas. Many of these have not only been expanded, but threshold requirements have been either lowered or removed for many types of searches by broadening the scope of the Foreign Intelligence Surveillance Act (FISA). Additionally, judicial approval for many searches has been reduced to a rubber stamp if the request is properly submitted.

A great deal of the USAPA focuses on the Internet.[21] This may be due to the extreme danger cyber crimes pose to the economy and to the Department of Defense (DOD), which maintains a network of over two

---

14. *See* Hentoff, *supra* note 7, ¶ 5.
15. *Id.* ¶ 7.
16. *Id.* ¶ 6.
17. *Id.* ¶ 9.
18. Scheer, *supra* note 11, ¶ 7.
19. Donohue & Walsh, *supra* note 12.
20. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).
21. *See generally* USAPA, Pub. L. No. 107-56, 115 Stat. 272 (2001).

million computers, 10,000 local area networks, and 100 long-distance networks, which handle 95% of military communications.[22] In 1999 alone the DOD was the target of 22,126 detected attacks, which may have represented only a small percentage of actual intrusions.[23] Nearly all of the attempted unauthorized entries were the work of "fledgling hackers" who target the DOD because of the prestige of evading its protections.[24] But whether hackers or terrorists, the danger is real.

One example occurred in 1997, when a teen hacker disrupted a telephone loop in Massachusetts, interrupting telephone service in hundreds of homes as well as the control tower at Worcester Airport.[25] Several hours passed before technicians could locate the problem, and it took more than a year to implement countermeasures.[26] Another example occurred in 1994, when two hackers breached an Air Force computer network at a research facility in upstate New York.[27] The hackers were not detected for five days, and repeatedly breached the network over a period of several months.[28] Investigators followed the trail to multiple locations around the United States, South America and, finally, Great Britain.[29] These hackers entered multiple government facilities, including NASA, and several private entities such as defense contractors, and downloaded sensitive information.[30] The cost of responding to this intrusion was estimated at half a million dollars.[31]

The dangers of cyber crime are difficult to overstate. Though not agents of any hostile power, many amateur hackers will publish the classified information that they are able to access in order to demonstrate their hacking abilities.[32] This permits the information to be accessed by anyone, including potential enemies. Also, terrorists could disrupt military operations by substituting munitions orders for other supplies such as light bulbs, thereby rendering military installations unprepared for combat.[33]

---

22. Lt. Col. Joginder S. Dhillon & Lt. Col. Robert I. Smith, *Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques,* 50 A.F. L. REV. 135, 140 (2001).

23. *See id.* The Defense Information Systems Agency (DISA) routinely conducts attacks on the military's computer networks to gauge their vulnerability. *Id*. Of 38,000 attempts by DISA, nearly two out of three were successful, and, of these, only four percent of the unauthorized intrusions were detected by the DOD. *Id.*

24. *Id.* at 141.

25. *Id.* at 141-42.

26. *Id.* at 142.

27. *Id.*

28. *Id.*

29. *Id.*

30. *Id.* at 143.

31. *See id*.

32. *Id.* at 141.

33. *Id.* at 144.

According to the FBI, in addition to the threat to national defense, electronic crime costs more than ten billion dollars per year.[34] Many businesses that are targeted never realize that they have been victimized, and of those, many simply do not report the crimes for fear of negative publicity.[35] The perpetrators of electronic crimes are elusive and may operate from anywhere in the world.

On October 26, 2001, at the signing of the USAPA, President Bush addressed the novel issues raised by new technology and the government's response:

> As of today, we're changing the laws governing information-sharing. And as importantly, we're changing the culture of our various agencies that fight terrorism. Countering and investigating terrorist activity is the number one priority for both law enforcement and intelligence agencies.
>
> Surveillance of communications is another essential tool to pursue and stop terrorists. The existing law was written in the era of rotary telephones. This new law that I sign today will allow surveillance of all communications used by terrorists, including e-mails, the Internet, and cell phones.
>
> As of today, we'll be able to better meet the technological challenges posed by this proliferation of communications technology. Investigations are often slowed by limits on the reach of federal search warrants. Law enforcement agencies have to get a new warrant for each new district they investigate, even when they're after the same suspect.
>
> Under this new law, warrants are valid across all districts and across all states.[36]

The Fourth Amendment requires that a search warrant specify the "place to be searched."[37] In order to search a place other than that specified, a new search warrant typically must be obtained.[38] While the primary effect of this "particularity" requirement is to eliminate general warrants, it also prevents law enforcement authorities from "forum

---

34. *Id.* at 139.

35. *Id.* at 140.

36. George W. Bush, Address at the White House signing of the USA PATRIOT Act of 2001 (Oct. 26, 2001), *available at* http:www.pbs.org/newshour/bb/terrorism/bush_terrorismbill.html.

37. U.S. CONST. amend. IV.

38. *How the USA-PATRIOT Act Limits Judicial Oversight of Telephone and Internet Surveillance,* ACLU FREEDOM NETWORK ¶ 7 (Oct. 23, 2001), *at* http://www.aclu.org/congress/l102301g.html [hereinafter *Judicial Oversight*].

shopping" by only giving the judge in the relevant jurisdiction the discretion to grant or deny the request for a warrant.[39] But, section 216 of the USAPA[40] permits a judge or magistrate to issue a pen register or trap and trace order that does not specify the Internet service provider (ISP), leaving it to the law enforcement officer to insert one or more ISPs of his choice.[41] This order is valid anywhere in the United States.[42] An ancillary effect of this provision is that if an ISP challenges the effect of the order, it must present the challenge in the jurisdiction where the order was issued, which could be across the country.[43] With little to gain, few ISPs are likely to bring such a challenge.[44]

In *Smith v. Maryland*,[45] the Supreme Court ruled that the installation and use of a pen register was not a search under the Fourth Amendment.[46] A pen register is defined as "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released."[47] In *Smith*, the defendant appealed his robbery conviction that was based on incriminating telephone company records.[48] Following the robbery, the defendant had made repeated telephone calls to his victim.[49] Based on information obtained from the

---

39. *See id.*

40. USAPA, Pub. L. No. 107-56, § 216, 115 Stat. 272 (2001). Section 216 (b)(1)(a)(1) reads:

> (1) Attorney for the government.—Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

*Id*.

41. *Judicial Oversight, supra* note 38, ¶ 8.
42. *Id.*
43. *See id.*
44. *See id.*
45. 442 U.S. 735 (1979).
46. *Id.* at 745-46.
47. *Id.* at 736 n.1.
48. *Id.* at 737-38.
49. *Id*. at 737.

telephone company pen register, police obtained a search warrant for his residence that yielded incriminating evidence.[50]

On appeal, the defendant sought to exclude "all fruits derived from the pen register"[51] because the police installed the device without a warrant.[52] The Court, in a 5-4 decision, held that there was "no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the Fourth Amendment."[53]

Before the passage of the USAPA, there was considerable debate about the applicability of the *Smith* pen register categorization to the Internet. Section 216 of the USAPA simply inserts the appropriate language to analogize the routing of electronic communications on the Internet to the dialing of a phone.[54] This permits enforcement officials to obtain such information as web addresses, e-mail addresses, and session times based on a lower standard than the probable cause necessary for a search warrant; the agent must merely certify that the information is "relevant to an ongoing criminal investigation."[55] The USAPA obligates the court to issue the warrant if this basic requirement is met.[56]

---

50. *Id.*

51. *Id*.

52. *Id.*

53. *Id.* at 738. The Court relied on the two-pronged analysis of subjective and objective expectations of privacy that was applied in *Katz v. United States,* 389 U.S. 347 (1967). *Id.* at 739-40; *see also* Rakas v. Illinois, 439 U.S. 128, 143, & n.12 (1978); *id.* at 150, 151 (Powell, J., concurring); *id.* at 164 (White, J., dissenting); United States v. Chadwick, 433 U.S. 1, 7 (1977); United States v. Miller, 425 U.S. 435, 442 (1976); United States v. Dionisio, 410 U.S. 1, 14 (1973); Couch v. United States, 409 U.S. 322, 335-36 (1973); United States v. White, 401 U.S. 745, 752 (1971) (stating a plurality opinion); Mancusi v. DeForte, 392 U.S. 364, 368 (1968); Terry v. Ohio, 392 U.S. 1, 9 (1968).

54. USAPA, Pub. L. No. 107-56, § 216, 115 Stat. 272 (2001). Section 216, MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES, reads:

> (a) General Limitations.—Section 3121(c) of title 18, United States Code, is amended—
>
> (1) by inserting "or trap and trace device" after "pen register";
>
> (2) by inserting, "routing, addressing," after "dialing"; and
>
> (3) by striking "call processing" and inserting "the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications."

*Id*. § 216(a)(1)-(3).

55. *Judicial Oversight, supra* note 38, ¶ 3.

56. USAPA, Pub. L. No. 107-56, § 216. The section reads:

> Upon an application made under section 3122(a)(1), the court *shall* enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for

But the analogy to telephone records is flawed. In order to appreciate the distinction, a basic understanding of the Internet is helpful. Rather than directly linking all of the computers of users, the Internet is able to function as it does by employing a technology known as packet switching.[57] This technology breaks data down into small packets of information, which are then transmitted and reassembled in the correct order at the destination computer.[58] The packets are encoded at the source for correct reassembly, permitting them to utilize the most efficient routing along the way.[59]

The *Smith* opinion, citing *United States v. New York Telephone Co.*,[60] reasoned that pen register-supplied information was not private because "[i]t does not overhear oral communications and does not indicate whether calls are actually completed."[61] Conversely, because the information contained in e-mail messages is transmitted in packets, whoever intercepts the message must separate the address from the contents of the e-mail.[62] The FBI responds to invasion of privacy concerns by asserting that they can be trusted to separate address from content and retain only the former.[63]

Perhaps the *Smith* decision would have been different if telephone numbers were spoken into the receiver, rather than dialed, and law enforcement officials had to separate the numbers from the remainder of the conversation.[64] Even without these issues, the *Smith* dissent was bitter in its concern for Fourth Amendment guarantees.[65] Justices Stewart and Brennan worried that "[t]he information captured by such surveillance emanates from private conduct within a person's home or office—locations that without question are entitled to Fourth and

---

> the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

*Id*. § 216(b)(1) (emphasis added).

57. Dhillon & Smith, *supra* note 22, at 138.

58. *Id.*

59. *See id.*

60. 434 U.S. 159 (1977).

61. Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979) (quoting *New York Tel. Co.*, 434 U.S. at 161 n.1).

62. *Judicial Oversight, supra* note 38, ¶ 5.

63. *Id.*

64. *See Smith*, 442 U.S. at 741. "[A] pen register differs significantly from the listening device employed in *Katz* [(Katz v. United States, 389 U.S. 347 (1967) (ruling that a wiretap of telephone booth was a search))], for pen registers do not acquire the *contents* of communications." *Id.*

65. *See id*. at 747 (Stewart, J., dissenting).

Fourteenth Amendment protection."[66] The *Smith* case has been frequently criticized for its narrowing of the expectation of privacy.[67]

The *Smith* opinion's analysis of the subjective expectation of privacy[68] takes on a new irony in light of the provisions of the USAPA. While discussing whether an individual's expectation of privacy is "reasonable," "legitimate," or "justifiable,"[69] the Court hypothesized a situation where a subjective expectation would not suffice as a standard for reasonableness.

> Situations can be imagined, of course, in which *Katz'* two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.[70]

---

66. *Id.* (Stewart, J., dissenting).

67. *See, e.g.,* People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983) ("A telephone subscriber . . . has an actual expectation that the dialing of telephone numbers from a home telephone will be free from governmental intrusion."); CLIFFORD S. FISHMAN, WIRETAPPING AND EAVESDROPPING § 28.1, at 279 (Cummulative Supp. 1994) ("unrestricted use of pen registers by the police would have a substantial and deleterious effect on privacy"); WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7, at 153-55 (Supp. 1986) (contending that individuals have a legitimate expectation of privacy in telephone records); Comment, *Pen Registers After* Smith v. Maryland, 15 HARV. C.R.-C.L. L. REV. 753 (1980).

68. *Smith,* 492 U.S. at 740.

69. *Id.* The Court cites as examples: *Rakas v. Illinois*, 439 U.S. 128, 143, & n.12 (1978); *id.* at 150, 151 (Powell, J., concurring); *id*. at 164 (White, J., dissenting); *United States v. Chadwick*, 433 U.S. 1, 7 (1977); *United States v. Miller*, 425 U.S. 435, 442 (1976); *United States v. Dionisio*, 410 U.S. 1, 14 (1973); *Couch v. United States*, 409 U.S. 322, 335-36 (1973); *United States v. White*, 401 U.S. 745, 752 (1971) (providing a plurality opinion); *Mancusi v. DeForte*, 392 U.S. 364, 368 (1968); and *Terry v. Ohio*, 392 U.S. 1, 9 (1968). *Smith*, 492 U.S. at 740.

70. *Id.* at 741 n.5.

With the enactment of the USAPA, the government has enacted such provisions, many of which are being criticized as "alien to well-recognized Fourth Amendment freedoms."[71] Considering that today many people maintain their "papers and effects" on their computer hard drives, the expansion of pen register authority to include electronic communications and Internet usage can "mean the collection of information more private than IP addresses, which are roughly the Net's equivalent of phone numbers."[72]

Attorney General John Ashcroft argues that roving wiretaps, which are permitted by section 206 of the USAPA,[73] do not violate the Fourth Amendment because they "do not eliminate the particularity requirement[s] for search warrants; [they] merely substitute particularity of person for particularity of place."[74] The Government contends that it will concentrate its surveillance only on the target of the investigation, but in reality all conversations, including those conducted by third parties, will be wiretapped.[75] To use one example, "if the government suspects that a particular target uses different pay phones at Boston's Logan Airport, then the government would have the power to wire all the public telephones at Logan Airport and the discretion to decide which conversations to monitor."[76]

In *Steagald v. United States*,[77] police

> relied on the warrant (arrest warrant for Ricky Lyons) as legal authority to enter the home of a third person based on their belief that Ricky Lyons might be a guest there . . . . [W]hile the warrant in this case may have protected Lyons from an unreasonable seizure, it did absolutely nothing to protect

---

71. *Id.*

72. Olsen, *supra* note 13, ¶ 14.

73. USAPA, Pub. L. No. 107-56, § 206, 115 Stat. 272 (2001). Section 206, ROVING SURVEILLANCE AUTHORITY UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, reads:

> Section 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)(2)(B)) is amended by inserting, "or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons," after "specified person."

*Id.*

74. Tracey Maclin, *On Amending the Fourth: Another Grave Threat to Liberty,* NAT. L. J., Nov. 12, 2001, at A20, *available at* http://www.law.com.

75. *See id.*

76. *Id.*

77. 451 U.S. 204 (1981).

> petitioner's privacy interest in being free from an unreasonable invasion and search of his home.[78]

Not only do roving telephone wiretaps invade the expectation of privacy of uncounted third parties, but the extension of roving surveillance to the computer equipment of a target also subjects "the e-mail messages of thousands of individuals" to government search.[79] Because government agents can now decide when, where, and how often to monitor communications, *Steagald* strongly suggests that this expansion of the government's power to monitor its citizens runs counter to the Fourth Amendment, which "was intended to check, and not expand, police power and discretion."[80]

The USAPA achieves a great deal of its expansion of investigative authority by making changes to the Foreign Intelligence Surveillance Act (FISA).[81] The FISA formerly granted FBI agents expanded authority to conduct warrantless surveillance, provided that *the purpose* of the investigation is to obtain "foreign intelligence information."[82] The FISA defines "foreign intelligence information" as:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.[83]

78. *Id.* at 213 (explanation added).
79. Maclin, *supra* note 74.
80. *Id.*
81. 50 U.S.C. § 1801 (2000).
82. *See id.* § 1802.
83. *Id.* § 1801(e).

Section 218 of the USAPA amends the criteria for FISA authority by "striking 'the purpose' and inserting 'a significant purpose'"[84] of the investigation, meaning any relation of the investigation to foreign intelligence is enough. This permits law enforcement agents to obtain expanded authority to conduct surveillance under the FISA by merely asserting that the investigation had something to do with foreign intelligence.[85]

The FISA was enacted in 1978 to provide a "firewall" between foreign and domestic intelligence gathering after the nation was shocked by revelations of extensive surveillance of U.S. citizens by the FBI, often on the basis of ethnicity or political beliefs.[86] During the 1960s and 1970s, the FBI conducted controversial surveillance of Vietnam War and civil rights protesters, including Martin Luther King.[87] By requiring that the primary purpose of a wiretap or search was to obtain foreign intelligence, the FISA forbade the use of the surveillance authority in criminal cases without meeting the probable cause standard.[88] Supporters of the USAPA cite *United States v. Truong Dinh Hung*[89] in their claim that President Carter "personally authorized warrantless physical searches by the FBI."[90] But the court made it clear in *Truong* that "once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution."[91] The expanded authority granted by the USAPA is certain to resurrect the practice of investigating Americans with unpopular political views, the same practice that prompted the original limiting language in the FISA.[92]

---

84. USAPA, Pub. L. No. 107-56, § 218, 115 Stat. 272 (2001). Section 218 reads: "Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking 'the purpose' and inserting 'a significant purpose.'" *Id*.

85. *See id*.

86. *How the USA-Patriot Act Enables Law Enforcement to Use Intelligence Authorities to Circumvent the Privacy Provisions Afforded in Criminal Cases,* ACLU Freedom Network ¶¶ 1-2 (Oct. 23, 2001), *at* http://www.aclu.org/congress/l102301i.html [hereinafter, *Intelligence Authorities*].

87. *Id.* ¶ 2.

88. *Id.* ¶ 3.

89. 629 F.2d 908 (4th Cir. 1980).

90. *See, e.g.,* U.S. Senate Republican Policy Committee, *The Anti-Terrorist Bill in Context: Is Safety a Civil Right?* ¶ 8 (Oct. 26, 2001), *at* http://www.senate.gov/~rpc/releases/1999/fr102601.htm.

91. *Truong*, 629 F.2d at 915.

92. *See generally Intelligence Authorities, supra* note 86.

Following passage of the USAPA, Senator Patrick Leahy, Chairman of the Senate Judiciary Committee, observed that "[t]he bill enters new and uncharted territory by breaking down traditional barriers between law enforcement and foreign intelligence."[93] Even under the pre-USAPA constraints, FISA wiretaps exceeded the number of wiretaps for all domestic criminal investigations combined.[94]

Another power given to the government is the "Authority to Share Grand Jury Information" granted by section 203 of the USAPA.[95] Grand juries have vast power to gather information in secret, "including testimony, wiretap transcripts, phone records, business records or medical records."[96] Section 203 amends Rule 6(e) of the Federal Rules of Criminal Procedure[97] to eliminate the need for a court order to permit prosecutors to share grand jury information with other government agencies.[98] Therefore, the FBI can now give grand jury information to the CIA without a court order.[99] As long as the information involves a non-American or involves "foreign intelligence," agencies can distribute, without limitation, information gathered about Americans.[100]

Finally, section 213 of the USAPA permits agencies to execute so-called "sneak and peek" warrants without notifying the target of the search.[101] This section expands the ability of the government to conduct

---

93. McGee, *supra* note 6 (quoting Senator Leahy).

94. *See USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances: An ACLU Legislative Analysis*, ACLU FREEDOM NETWORK ¶ 16 (Nov. 1, 2001), *at* http://www.aclu.org/congress/l110101a.html [hereinafter *Checks and Balances*].

95. USAPA, Pub. L. No. 107-56, § 203(a), 115 Stat. 272 (2001).

96. McGee, *supra* note 6.

97. FED. R. CRIM. P. 6(e).

98. McGee, *supra* note 6.

99. *Id.*

100. *Id.*

101. USAPA, Pub. L. No. 107-56, § 213, 115 Stat. 272 (2001). Section 213, AUTHORITY FOR DELAYING NOTICE OF THE EXECUTION OF A WARRANT, provides that:

> Section 3103a of title 18, United States Code, is amended—
>
> (1) by inserting "(a) In General."—before "In addition"; and
>
> (2) by adding at the end the following:
>
> (b) Delay—With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if—
>
> (1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);
>
> (2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly

secret "black bag" searches in every criminal case.[102] Under the USAPA the government need only assert that notice "may" seriously jeopardize an investigation.[103]

The result of this provision is that citizens are not provided with notice of a search warrant and, therefore, have no opportunity to contest the warrant's validity or accuracy before an intrusion of their home or office occurs.[104] Considering the possibility of the police showing up at the door with a warrant to search one's house, Senator Feingold commented,

> You look at the warrant and say, "yes, that's my address, but the name on the warrant isn't me." And the police realize a mistake has been made and go away. If you're not home, and the police have received permission to do a "sneak and peek" search, they can come into your house, look around, and leave, and may never have to tell you.[105]

As one commentator put it, "[t]hese so-called 'sneak and peek' provisions treat the Fourth Amendment protections as if they were written in pencil, easily erased and malleable, tied to the crisis-of-the-day level of paranoia."[106]

## III. HISTORY OF CRISIS LEGISLATION

> When I think of the progress we have made over the last thirty years, I look upon our system of civil liberties with some satisfaction, and a certain pride. There is considerably less to be proud about, and a good deal to be embarrassed about, when one reflects on the shabby treatment civil

---

> provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and
>
> (3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.

*Id*.

102. *See Checks and Balances, supra* note 94, ¶ 7.

103. Senator Russell Feingold, Statement on the Anti-Terrorism Bill from the Senate Floor (Oct. 25, 2001), *available at* http://feingold.senate.gov/releases/01/10/102501at.html [hereinafter *Feingold Statement*].

104. *Id.*

105. *Id.*

106. Brock N. Meeks, *First, Brand All the Children: Cyber-liberties Swept Away by Tidal Wave of Security Concerns* ¶ 8 (Oct. 24, 2001), *at* http://www.msnbc.com/news/646793.asp.

> liberties have received in the United States during times of war and perceived threats to its national security.[107]
>
> -Justice William Brennan, 1987

In 1798, the Alien Enemies Act permitted the President of the United States to "order all such aliens as he shall judge dangerous to the peace and safety of the United States, or shall have reasonable grounds to suspect are concerned in any reasonable or secret machinations against the government thereof, to depart out of the territory of the United States."[108] The "Alien and Sedition Acts," prompted by the imminent prospect of war with France, made it illegal to "'write, print, utter or publish . . . any false, scandalous and malicious writing . . . against' the U.S. Government, Congress, or the President [if accompanied by] the intent 'to bring them . . . into contempt or disrepute.'"[109] This statute, written "[w]hen the ink had barely dried on the First Amendment,"[110] permitted the government to stifle and punish political opposition. It was the natural product of a new nation, unsure of its continued existence and lacking a history of jurisprudence to rely upon for guidance.[111] After the crisis had passed, all those convicted under the Alien and Sedition Acts were pardoned by President Jefferson, and Congress repaid most of their fines.[112] But events would soon show that America had not learned from the experience.

Shortly after the outbreak of the Civil War, President Lincoln suspended the writ of habeas corpus and had between 20,000 and 30,000 persons arrested and detained by military personnel without charges.[113] Some received no trials; all were held at the whim of authorities, lacking any access to the due process guarantees provided by civil courts.[114] The American public was strongly in favor of these actions, but in *Ex parte Merryman*,[115] Chief Justice Taney found them to be unconstitutional.[116]

---

107. Justice William J. Brennan, Jr., The Quest to Develop a Jurisprudence of Civil Liberties in Times of Security Crisis, Address to the Law School of Hebrew University, Jerusalem, at 1 (Dec. 22, 1987), *available at* http://www.brennancenter.org/resources/downloads/nation-security-brennan.pdf.

108. Alien Enemies Act, ch. 58, 1 Stat. 570 (1798) (emphasis omitted); *see also* Anita Ramasastry, *Indefinite Detention Based Upon Suspicion: How the Patriot Act Will Disrupt Many Lawful Immigrants' Lives* ¶ 27 (Oct. 25, 2001), *at* http://writ.news.findlaw.com/commentary/20011005_ramasastry.html.

109. Brennan, *supra* note 107, at 2 (omissions in original) (footnote omitted).

110. *Id.*

111. *See id.*

112. *Id.* at 3.

113. *Id.*

114. *Id.*

115. 17 F. Cas. 144 (C.C.D. Md. 1861) (No. 9,487).

116. Brennan, *supra* note 107, at 3.

Chief Justice Taney was subsequently accused by the press of siding with traitors.[117] The *New York Tribune* wrote, "[w]hen reason stalks about in arms, let decrepit Judges give place to men capable of detecting and crushing it."[118] After the war was over, cooler heads prevailed, and in *Ex parte Milligan*[119] the Court ruled that it is unconstitutional to establish a system of military tribunals and suspend habeas corpus in any locality where civil courts are open and functioning.[120] This was to represent America's equal application of civil liberties to both times of war and times of peace.[121]

This lofty aspiration lasted until the next big scare.[122] The Espionage Act of 1917[123] criminalized the publication of any false material that might endanger the success of U.S. military operations or recruiting, and allowed for the confiscation of any such materials.[124] This Act provided a vehicle for the government to confiscate anti-war films and literature.[125] Later the statute was expanded to include the willful publication, utterance, writing or printing of "disloyal, profane, scurrilous, or abusive language about the U.S. form of government, Constitution, flag, or its military forces or uniform."[126]

The Espionage Act of 1917 was no mere exercise in rhetoric: over 2,000 individuals were prosecuted under the Act, mainly for criticizing the war or for the act of contradicting statements made by President Wilson.[127] Other offenders ran afoul of the Act by making statements on such diverse subjects as religion, taxation, and the draft.[128]

The internment of 120,000 Japanese citizens during the Second World War is a more recent, and therefore more nagging instance of a measure that was necessitated by an imminent threat to national security—in this case the presence on American soil of disloyal Japanese-Americans.[129] Although the Supreme Court refused to second-guess the exigencies of national security in *Hirabayashi v. United States*,[130] the action was later

117. *Id.*
118. *Id.*
119. 71 U.S. (4 Wall.) 2 (1866).
120. Brennan, *supra* note 107, at 3.
121. *Id.*
122. *Id.*
123. Pub. L. No. 65-24, 40 Stat. 217 (1917).
124. Brennan, *supra* note 107, at 3.
125. *Id.*
126. *Id*. (citations omitted).
127. *Id.*
128. *Id.* at 4-5.
129. *Id.* at 6; *see also* Hirabayashi v. United States, 828 F.2d 591, 598 (9th Cir. 1987).
130. 320 U.S. 81 (1943). The Court stated:

found to be without factual basis. "[I]n 1980 Congress established the Commission on Wartime Relocation and Internment of Civilians, which reviewed all the evidence and concluded that . . . a grave injustice" had been committed, "not justified by [any] military necessity," but rather the product of "race prejudice, war hysteria and a failure of political leadership."[131] The Commission authorized reparations for those affected.[132]

The arrival of the Nuclear Age prompted another era of national anxiety, this time in response to the Red Menace.[133] To protect the nation from the threat within, Congress "enacted various laws including the Internal Security Act of 1950 and the Communist Control Act of 1954."[134] In *Dennis v. United States*,[135] the Supreme Court, using the "clear and present danger" test,[136] upheld the conviction of Communist Party members. The Court ruled that a finding of this "clear and present danger" subordinated any constitutional rights of free speech and assembly.[137]

## IV. CONCLUSION

> In the play, "A Man for All Seasons," Sir Thomas More questions the bounder Roper whether he would level the forest of English laws to punish the Devil. "What would you do?" More asks, "Cut a great road through the law to get after the Devil?" Roper affirms, "I'd cut down every law in England to do that." To which More replies:

---

> we cannot reject as unfounded the judgment of the military authorities and of Congress that there were disloyal members of that population, whose number and strength could not be precisely and quickly ascertained. We cannot say that the war-making branches of the Government did not have ground for believing that in a critical hour such persons could not readily be isolated and separately dealt with, and constituted a menace to the national defense and safety, which demanded that prompt and adequate measures be taken to guard against it.

*Id.* at 99.

131. Brennan, *supra* note 107, at 6 (quotation marks omitted).

132. *See* 50 USCS Appx § 1989 (1988) (providing apology and restitution for the internment of citizens and permanent aliens of Japanese ancestry).

133. *See* Brennan, *supra* note 107, at 7.

134. *Id.* at 7.

135. 341 U.S. 494 (1951).

136. *Id*. at 515. The "clear and present danger" test was formulated in *Schenk v. United States*, 249 U.S. 47 (1919). In *Schenck*, the defendant and others were convicted of conspiracy to violate the Federal Espionage Act of 1917 for distributing leaflets that promoted military insubordination and the obstruction of military recruitment. *Id.* at 47-48. Utilizing the "clear and present danger" balancing test, the Supreme Court affirmed the convictions. *Id.* at 52-53.

137. *See Dennis*, 341 U.S. at 513.

> "And when the last law was down, and the Devil turned round on you—where would you hide, Roper, the laws all being flat? This country's planted thick with laws from coast to coast . . . and if you cut them down . . . d'you really think you could stand upright in the winds that would blow then? Yes, I'd give the Devil benefit of law, for my own safety's sake."[138]

Among the myriad troubling questions associated with the USAPA, the most fundamental is whether there was a need for it at all. The government never argued that the legal restraints on law enforcement authorities prevented them from stopping the terrorists of September 11th, or from investigating the crime.[139] The FBI already had the power and the technology to monitor telephone and Internet communications in situations involving air piracy and the destruction of aircraft,[140] as well as under the FISA.[141] Existing law provided for roving wiretaps if law enforcement agents could demonstrate that the target of the investigation was changing phones in order to thwart detection.[142] The government could already wiretap any person suspected of working for a foreign government or organization.[143] The government already had "sneak and peek" authority to search without notification, if certain criteria were met: if an agent demonstrated that either an individual's safety would be endangered, someone would flee, evidence would be destroyed, witnesses would be intimidated or an investigation would otherwise be jeopardized or delayed, this authority could be granted.[144]

One of the most far-reaching effects of the USAPA is the removal of the review of a "neutral and detached magistrate" from the process of citizen surveillance. Many of the provisions that do involve some judicial oversight require that the order be granted if the application is properly filled out.[145] Under the broader FISA provisions that now apply to the investigation of domestic crimes under the USAPA, no probable cause is necessary to justify an intelligence wiretap.[146]

---

138. *Feingold Statement*, *supra* note 103.

139. *EEF Analysis of the Provisions of the USA PATRIOT Act That Relate to Online Activities*, ¶¶ 3, 36-38, 43, 46, 49, 51-52, 54 (Oct. 31, 2001), *at* http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html.

140. *Judicial Oversight, supra* note 38, ¶ 2.

141. *Checks and Balances, supra* note 94, ¶ 15.

142. *Judicial Oversight, supra* note 38, ¶ 10.

143. Ramasastry, *supra* note 108, ¶ 24.

144. *How the USA-Patriot Act Expands Law Enforcement "Sneak and Peek" Warrants,* ACLU Freedom Network ¶¶ 2, 4 (Oct. 23, 2001), *at* http://www.aclu.org/congress/l102301b.html.

145. *See, e.g., Intelligence Authorities, supra* note 86, ¶ 13.

146. *Judicial Oversight, supra* note 38, ¶ 4.

Many of the provisions of the USAPA are disturbingly vague. Section 808 expands the definition of terrorism to crimes "relating to protection of computers."[147] This language could encompass a wide range of offenses unrelated to terrorism, such as the sale of software that fails to perform correctly, posting incorrect or misleading content on web pages, and

147. USAPA, Pub. L. No. 107-56, § 808, 115 Stat. 272 (2001). Section 808, DEFINITION OF FEDERAL CRIME OF TERRORISM, reads in part:

> Section 2332b of title 18, United States Code, is amended—
>
> (1) in subsection (f), by inserting "and any violation of section 351(e), 844(e), 844(f)(1), 956(b), 1361, 1366(b), 1366(c), 1751(e), 2152, or 2156 of this title," before "and the Secretary"; and
>
> (2) in subsection (g)(5)(B), by striking clauses (i) through (iii) and inserting the following:
>
> (i) section 32 (relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 or 175b (relating to biological weapons), 229 (relating to chemical weapons), subsection (a), (b), (c), or (d) of section 351 (relating to congressional, cabinet, and Supreme Court assassination and kidnaping), 831 (relating to nuclear materials), 842(m) or (n) (relating to plastic explosives), 844(f)(2) or (3) (relating to arson and bombing of Government property risking or causing death), 844(i) (relating to arson and bombing of property used in interstate commerce), 930(c) (relating to killing or attempted killing during an attack on a Federal facility with a dangerous weapon), 956(a)(1) (relating to conspiracy to murder, kidnap, or maim persons abroad), 1030(a)(1) (relating to protection of computers), 1030(a)(5)(A)(i) resulting in damage as defined in 1030(a)(5)(B)(ii) through (v) (relating to protection of computers), 1114 (relating to killing or attempted killing of officers and employees of the United States), 1116 (relating to murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (relating to hostage taking), 1362 (relating to destruction of communication lines, stations, or systems), 1363 (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States), 1366(a) (relating to destruction of an energy facility), 1751(a), (b), (c), or (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1992 (relating to wrecking trains), 1993 (relating to terrorist attacks and other acts of violence against mass transportation systems), 2155 (relating to destruction of national defense materials, premises, or utilities), 2280 (relating to violence against maritime navigation), 2281 (relating to violence against maritime fixed platforms), 2332 (relating to certain homicides and other violence against United States nationals occurring outside of the United States), 2332a (relating to use of weapons of mass destruction), 2332b (relating to acts of terrorism transcending national boundaries), 2339 (relating to harboring terrorists), 2339A (relating to providing material support to terrorists), 2339B (relating to providing material support to terrorist organizations), or 2340A (relating to torture) of this title.

*Id.* § 808(1)-(2)(i).

deceptive Internet marketing schemes.[148] While these all may be serious problems, they do not merit the abrogation of constitutional liberties.

Many critics question the motivation behind the USAPA. Senator Feingold said that the USAPA "goes into a lot of areas that have nothing to do with terrorism and have a lot to do with the government and the FBI having a wish list of things they want to do."[149] A principal concern of critics is the broad expansion of FISA surveillance authority, allowing its use in primarily criminal investigations.[150] This has the effect of converting the FBI's mission from solving crime to intelligence gathering, and effectively "put[s] the CIA back in the business of spying on Americans."[151] The USAPA also creates the new crime of "domestic terrorism"[152] that could transform protesters into terrorists if they are associated with conduct that endangers human life.[153]

Others are skeptical about the promised benefit of increased security. Carole Samdup, spokesperson for Democracy and Rights, claims "[a]ll this technology has existed for years and we still haven't arrested anyone (using it) . . . . Even Timothy McVeigh was under surveillance."[154] Boaz Guttman, former terrorism investigator in the Israeli police force, downplays the utility of technologies such as Carnivore, a program that monitors and filters all electronic communications in search of particular terms.

> There is no miracle at all with wiretapping. It did not prevent crime even in Red Russia. What if terrorists use coded messages. He [sic] calls the bomb "cake" and the target "my mother in law." You can intercept 'til tomorrow, 'til next week [and not stop terrorism] . . . . If somebody thinks that with all this tracing alone, he will defeat terror, as I said to an important person in your country, "Sorry, you are sleeping in the middle of the day."[155]

More fundamentally, the focus of the USAPA on expanding government surveillance is misguided, because the underlying assumption

---

148. Susan Evoy, *Comments on Legislative Proposals to Protect National Security and Their Impact on the Communications Infrastructure,* COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY ¶ 8 (Oct. 2001), *at* http://www.cpsr.org/issues/ICACComments.html (last visited Dec. 11, 2001).

149. Hentoff, *supra* note 7, ¶ 20 (quoting Senator Feingold).

150. *Judicial Oversight, supra* note 38, ¶¶ 13-14.

151. *Checks and Balances, supra* note 94, ¶ 20.

152. USAPA, Pub. L. No. 107-56, § 802.

153. *Checks and Balances, supra* note 94, ¶¶ 8-9.

154. Bob Sullivan, *Warming to Big Brother,* MSNBC, ¶ 28, *at* http://www.msnbc.ru/news/654959 (last visited Dec. 12, 2001).

155. *Id.* ¶¶ 29, 31 (quotation marks omitted).

that the attacks of September 11 resulted from the government's limited power to collect information is erroneous. For example, after the 1993 bombing of the World Trade Center, the FBI discovered that it already had in its possession detailed plans and maps of the attack at the time it occurred.[156] The history of intelligence indicates that most failures result from a lack of proper implementation of procedures already in place, rather than the need for new procedures.[157]

No restraint was ever placed on government power without a history of government abuse. As far back as 1706 the Framers were aware of the dangers of multiple-specific search warrants, after colonial officials used them to search every home in New Hampshire.[158] Congressional concern led to the Collection Act of 1789, which limited federal searches to single structures and eliminated "wide-ranging exploratory searches."[159]

Because these limitations are intended to remedy government overreaching, no one ever proposes lifting governmental restraints until the memory of abuse has time to fade, usually a generation or two after the excesses. No doubt the future will bring vivid reminders of the original reasons for the restraints that Congress has so hastily lifted from the powers of the government over its citizens.

Ironically, blanket monitoring of citizens could have the same chilling effect on democracy that terrorism does.[160] Justice Marshall, dissenting in *Smith*, remarked that

> [p]ermitting governmental access to telephone records on less than probable cause may . . . impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society. Particularly given the Government's previous reliance on warrantless telephonic surveillance to trace reporters' sources and monitor protected political activity, I am unwilling to insulate use of pen registers from independent judicial review.[161]

One imagines what Justice Marshall would have said about the legislation before us.

Daniel Bryant, Assistant Attorney General for the Department of Justice, observed that "[a]s the Commander-In-Chief, the President must be able to use whatever means necessary to prevent attacks upon the United States; this power, by implication, includes the authority to collect

156. Donohue & Walsh, *supra* note 12.
157. *See id.*
158. Maclin, *supra* note 74.
159. *Id.*
160. Evoy, *supra* note 148, ¶ 7.
161. Smith v. Maryland, 442 U.S. 735, 751 (Marshall, J., dissenting) (footnote omitted).

information necessary for its effective exercise."[162] No one can gainsay this; however, the means utilized by the President must be subject to constitutional constraints.[163] The President is not above the law and not above the Constitution.[164]

Civil liberties are anathema to government. Since the first collectivization of humans, governments have jealously guarded their powers, only reluctantly ceding increments of control to their subjects. That is the miracle of America. In spite of historical excesses, this nation has always returned to the principles of human rights and guarantees envisioned by the Founding Fathers.

Justice Brennan, in his 1987 address to the Law School of Hebrew University in Jerusalem, expressed frustration at America's episodic abandonment of civil liberties in times of crisis.[165] Justice Brennan noted that "[a]fter each perceived security crisis ended, the United States has remorsefully realized that the abrogation of civil liberties was unnecessary. But it has proven unable to prevent itself from repeating the error when the next crisis came along."[166]

There is no doubt that the expanded powers incorporated into the USAPA will be used improperly, especially given the limited oversight provisions.[167] Political enemies will be targets of espionage;[168] embarrassing information about select individuals will once again be "leaked." Perhaps terrorists will even be freed after incriminating evidence is suppressed on constitutional grounds (if they manage to obtain a civil trial).[169]

Eventually, the stories of governmental excess will be publicized, and the public will realize the damage that has been done to personal privacy. This has already occurred with well-meaning legislation such as RICO[170] and other asset forfeiture provisions that have succeeded in injuring average citizens while failing to remedy the problems they were intended to address. History shows that individuals will suffer gravely before the damage is recognized, and once again America will realize that a society that sacrifices its freedom for security achieves neither.

---

162. *Intelligence Authorities, supra* note 86, ¶¶ 8-9.

163. *See id*. ¶ 10.

164. *Id.*

165. Brennan, *supra* note 107, at 1.

166. *Id.*

167. *See Intelligence Authorities, supra* note 86, ¶¶ 13-14.

168. *Id*. ¶ 15.

169. *Id*. ¶ 6.

170. *See, e.g.,* Alexander v. United States, 509 U.S. 544 (1993) (involving the seizure of an adult bookstore's assets under RICO forfeiture provisions).