

PATRIOT 2005–2007:
TRUTH, CONTROVERSY, AND CONSEQUENCES

RONALD J. SIEVERT*

I.	INTRODUCTION	320
II.	PROVISIONS DESIGNED TO INCREASE COMMUNICATION WITHIN GOVERNMENT	322
	A. <i>From Intelligence to Law Enforcement</i>	323
	B. <i>2005–2006 Allegations of Illegal Surveillance Against al Qaeda in the United States</i>	328
	C. <i>From Law Enforcement to Intelligence</i>	331
III.	WELCOME TO THE TWENTY-FIRST CENTURY: PROVIDING COMPUTER RECORDS TO INTELLIGENCE AND LAW ENFORCEMENT OFFICIALS	335
	A. <i>Computer Contact Information</i>	335
	B. <i>National Security Letters</i>	337
	C. <i>Content</i>	342
IV.	“SNEAK AND PEEK” WARRANTS	345
V.	ACCESS TO RECORDS	347
VI.	CONCLUSION	350

* Adjunct Professor, University of Texas at Austin School of Law, U.S. Law & National Security and Federal Criminal Law. Author, CASES AND MATERIALS ON U.S. LAW AND NATIONAL SECURITY (2000). Professor Sievert earned his B.A. from St. Bonaventure University in 1970 and his J.D. from The University of Texas at Austin School of Law in 1977. The following article reflects the opinions of the author and does not necessarily reflect the position of any United States government department or agency.

I. INTRODUCTION

For a number of years this nation was immersed in a Patriot Act¹ frenzy driven by conservative and liberal politicians, the media, and special interest groups. The frenzy was characterized by sound bites and headlines intended to have an impact on the public but which, unfortunately, often did not illuminate the facts or the actual law enacted by the Patriot Act. Politicians and pundits were quick to label the Act as either good for America and necessary for national security, or as an unconstitutional infringement on civil liberties,² consistently failing to reference or accurately describe the exact provisions that supported their conclusions.³

All of this, of course, took place in a highly charged atmosphere in which the very names “Patriot,” “Ashcroft,” “Gonzales,” and “Bush” brought forth images of right-wing ideologies bent on violating civil liberties to protect national security or increase their personal and partisan control over the government. This context, when added to the general ignorance of the Act, served to dramatically enhance the emotion and confusion that dominated the debate.

It is thus not surprising that one frequently encounters both citizens and lawyers who sincerely question “the Patriot Act,” but, when asked which sections bother them most, often refer to completely unrelated components of the administration’s war on terror. It has been common, for example, to hear complaints that it is improper for the Patriot Act to allow government

1. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 357 (2001) (codified in scattered sections of 8, 15, 18, 22, 31, 42, 49, and 50 U.S.C.) [hereinafter Patriot Act].

2. See, e.g., *Patriot Act Debate Continues: Bush Calls Senators Who Are Blocking Renewal of the Act ‘Irresponsible’*, CBSNEWS.COM, Dec. 17, 2005, <http://www.cbsnews.com/stories/2005/12/16/politics/main1132164.shtml> (quoting Senator Harry Reid’s statement that “when we start saying security is more important than the liberties of the American people this country is in trouble,” and Senator Patrick Leahy that the Patriot Act fell short of protecting basic civil liberties); *Patriot Act Renewal Fails in Senate: GOP Fights to Save Provisions Before End-of-Year Deadline*, CNN.COM, Dec. 16, 2005, <http://www.cnn.com/2005/POLITICS/12/16/patriot.act/> (quoting President Bush to the effect that the Patriot Act is “essential to fighting the war on terror and preventing our enemies from striking America again,” and Attorney General Alberto Gonzales stating that the Patriot Act is “essential to our efforts in the war on terrorism”).

3. This general statement is the main topic of this article.

monitoring of communications between an attorney and client. This procedure, however, stems from a 2001 order from the Attorney General to the Bureau of Prisons entitled “Monitoring of Attorney-Client Communications of Designated Federal Prisoners,”⁴ is based on a Supreme Court case,⁵ and is utilized only when the parties have been advised that their communications are subject to being monitored.⁶ Regardless of the advisability of the order, it is not connected with the Patriot Act. Citizens have also responded with references to the potential trial of terrorist suspects before military tribunals. These proceedings, however, are based on a 2001 presidential order entitled “Detention, Treatment, and Trial of Certain Non-Citizens in the War against Terrorism,”⁷ which in turn relies upon a number of Supreme Court cases,⁸ and, again, have no connection to the Patriot Act.

Perhaps of greater concern, as will be detailed at length in this article, is the fact that when those who raised serious questions managed to refer to legal concepts that actually are in the Patriot Act, such as “sneak and peak” warrants, the searching of business and computer records, or the Foreign Intelligence Surveillance Act (FISA),⁹ their characterizations of the statute’s provisions, relying as they did on political, media, and special interest sources, was in many cases extremely wide of the mark.¹⁰

4. Att’y Gen. Order No. 2529-2001, 66 Fed. Reg. 55,062 (Oct. 31, 2001).

5. *Weatherford v. Bursey*, 429 U.S. 545 (1977).

6. Att’y Gen. Order No. 2529-2001, *supra* note 4, at 55,064.

7. Military Order of Nov. 13, 2001, 66 Fed. Reg. 57,833 (Nov. 13, 2001).

8. *E.g.*, *Ex parte Quirin*, 317 U.S. 1, 2 (1942) (holding that the president was authorized to order a trial before a military commission and that it was lawful to keep defendants in custody prior to the trial); *see also* *Johnson v. Eisentrager*, 339 U.S. 763, 784–85 (1950) (stating that it is illogical to conclude that constitutional protections apply to nonresident enemy aliens given that even American soldiers do not have the right to jury trials). In *Hamdi v. Rumsfeld*, the Court noted that the standards articulated to designate enemy combatants could be met by “an appropriately authorized and properly constituted military tribunal.” 542 U.S. 507, 538 (2004). The Military Commissions Act of 2006 adopted the rules for military commissions to try defendants for violating the laws of war. Pub. L. No. 109-366, 120 Stat. 2600 (2006) (codified at 10 U.S.C. §§ 948a–950w (2006)).

9. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. §§ 1801–1871) (prior to 2001 and 2006 amendments) [hereinafter FISA].

10. This paragraph’s overview in part refers to those who raise sincere questions about the Patriot Act that do not actually reflect the wording or real meaning of the statute. These questions have been raised at a number of public seminars at which the author has been a speaker; these seminars will be referenced throughout this article and include the following: San Antonio City Council Meeting, Aug. 12, 2004; Texas State University-sponsored conference on the Patriot Act, Nov. 20, 2003; Austin City Council

During the last two years we have finally witnessed the submission of well-formulated legal challenges to the Patriot Act's actual provisions in the courts and before Congress. These challenges have resulted in initial legal opinions by the lower courts as well as amendments to the Act itself in the USA PATRIOT Improvement and Reauthorization Act of 2005 (PIRA)¹¹ and USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (Patriot Amendments Act).¹² Now, therefore, is a perfect time to step back and accurately examine the most controversial provisions of the Act and review what, if anything, has been done to modify those provisions.

II. PROVISIONS DESIGNED TO INCREASE COMMUNICATION WITHIN GOVERNMENT

During the aftermath of September 11th, commentators and politicians proclaimed that the reason for the success of the attacks was because the Federal Bureau of Investigation (FBI), whose focus is law enforcement, and Central Intelligence Agency (CIA), whose focus is intelligence, did not communicate with each other.¹³ If they had communicated, according to these critics, they certainly would have been able to "connect the dots" that stood out in isolated pieces of information known to some government agents but apparently not collected and understood by analysts in one central office.¹⁴ There is probably some truth to this general allegation, at least as it relates to lack of communication. The reason for this lack of communication was

Meeting, Sept. 25, 2003; ACLU-sponsored conference on the Patriot Act, University of Texas at Austin, Sept. 13, 2003; University of Texas at Austin-sponsored seminar entitled "Impact of Government's Anti-Terror Provisions on Civil Liberties," Feb. 28, 2003 [hereinafter Patriot Act Conferences & Meetings].

11. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006) (codified in scattered sections of 8, 15, 18, 21, 28, and 42 U.S.C.) [hereinafter PIRA].

12. USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, 120 Stat. 278 (2006) (codified in scattered sections of 8, 15, 18, 22, 31, 42, 49, and 50 U.S.C.) [hereinafter Patriot Amendments Act].

13. See, e.g., NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 78-80 (2004).

14. See, e.g., Editorial, *Terrifying Reading*, ST. PETERSBURG TIMES, Apr. 18, 2004, at P2 (pointing out "the FBI leadership's failure to connect the leads developed by field agents in the months prior to the 9/11 attacks"); *9/11 Chair: Attack Was Preventable: Head of Sept. 11 Panel Lays Blame Inside Bush Administration*, CBSNEWS.COM, Dec. 17, 2003, <http://www.cbsnews.com/stories/2003/12/17/eveningnews/main589137.shtml> ("[September 11th] widows want to know why various government agencies didn't connect the dots before Sept. 11, such as warnings from FBI offices in Minnesota and Arizona about suspicious student pilots.").

a combination of traditional government bureaucratic infighting and legislation that acted to ensure that government knowledge by any one individual was not easily accessible in one giant computer (as often depicted on television) so as to avoid federal “Big Brother”-like intrusion upon individual rights and privacy.¹⁵ The Patriot Act sought to eliminate some of these barriers through specific provisions designed to facilitate communication between the law enforcement and intelligence communities. This effort has naturally led to criticism by civil libertarians that “[t]he sharing of such a broad range of information raises the specter of intelligence agencies, once again, collecting, profiling and potentially harassing U.S. persons engaged in lawful . . . activities.”¹⁶ The accuracy of this criticism and related concerns can best be gauged by a review of the actual provisions.

A. From Intelligence to Law Enforcement

The Patriot Act attempted to increase the flow of information from the CIA and National Security Agency (NSA) to the FBI. As revealed by the Final Report of the Attorney General’s Review Team on the Handling of the Los Alamos National Laboratory Investigation, a wall had been erected between intelligence agencies and law enforcement during the 1980s.¹⁷ This wall was so impermeable, and its existence so ludicrous, that the head of the Department of Justice (DOJ) section responsible for prosecuting spies did not know that the CIA, FBI, and DOJ intelligence branches all had been investigating Wen Ho Lee for espionage activity until the whole case broke in the *New York Times*.¹⁸ In his testimony before the United States Senate Judiciary Committee, United States Attorney Patrick Fitzgerald discussed this problem in the context of his 1996 investigation of

15. The grand jury and FISA legislation referenced in this section of the article are examples of the past efforts to keep government information compartmentalized. The rules related to access and sharing of tax information within the government are also characteristic of the effort. For example, section 6103 of the Internal Revenue Code lays out extensive provisions restricting agency access to tax records, limiting disclosure of those records to others in the government when they are obtained, and mandating certain correlated reporting. 26 U.S.C. § 6103.

16. John Podesta, *USA Patriot Act: The Good, the Bad, and the Sunset*, A.B.A. SEC. OF INDIVIDUAL RTS. & RESPS., HUM. RTS. MAG., Winter 2002, at 3.

17. RANDY I. BELLOWS, U.S. DEP’T OF JUSTICE, FINAL REPORT OF THE ATTORNEY GENERAL’S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NATIONAL LABORATORY INVESTIGATION (May 2000), <http://www.usdoj.gov/ag/readingroom/bellows.htm>.

18. *Id.* at 688.

Osama Bin Laden and 1998 investigation of the U.S. embassy bombings in Africa, stating the following:

[We] began a criminal investigation of Usama Bin Laden in early 1996. The team—prosecutors and FBI agents assigned to the criminal case—had access to a number of sources. We could talk to citizens. We could talk to local police officers. . . . We could talk to foreign police officers. Even foreign intelligence personnel. And foreign citizens We could even talk to al Qaeda members. . . . But there was one group of people we were not permitted to talk to. Who? The FBI agents across the street from us in lower Manhattan assigned to a parallel intelligence investigation of Usama Bin Laden and al Qaeda. We could not learn what information they had gathered. That was “the wall.”¹⁹

This bureaucratic wall developed because of the difference in the predicates for a FISA wiretap (and search)²⁰ and a Title III criminal wiretap.²¹ When Congress passed FISA in 1978, it required, before conducting electronic surveillance in intelligence cases, that the government show “probable cause” that *the target is an “agent of a foreign power”* in order to obtain an intelligence wiretap.²² By contrast, the Title III standard to obtain a criminal wiretap is “probable cause” that *the target is “committing . . . a particular [criminal] offense.”*²³

Because, arguably, the intelligence standard is lower than the criminal standard, some courts attempted to ensure that intelligence surveillance was not used as a pretext to avoid the stricter demands for intercepts in criminal cases. These courts emphasized that under the statute, intelligence must be the primary purpose of the FISA wiretap.²⁴ The DOJ bureaucracy, led by the Office of Intelligence Policy and Review, out of an abundance of caution, took these cases to mean that there should be very little interaction between criminal divisions and

19. *Hearing on Protecting Our National Security from Terrorist Attacks: A Review of Criminal Terrorism Investigations and Prosecutions Before the S. Comm. on the Judiciary*, 108th Cong. 2 (2003) (statement of Patrick Fitzgerald, U.S. Attorney for the Northern District of Illinois).

20. 50 U.S.C. §§ 1804–1829 (1998).

21. 18 U.S.C. §§ 2517–2521.

22. 50 U.S.C. § 1805(a)(3)(A) (emphasis added).

23. 18 U.S.C. § 2518(3)(a) (emphasis added).

24. *See, e.g., United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) (holding that evidence obtained through warrantless surveillance conducted prior to the investigation becoming “primarily . . . criminal” was admissible, but that subsequent surveillance required a warrant).

intelligence agencies in any case where a FISA warrant might be obtained.²⁵ Out of further caution, this lack of communication eventually grew to the point that personnel at both the FBI and CIA believed there was to be almost no communication—period—during active investigations between intelligence agents (e.g., those working for the CIA and FBI counter-espionage effort) and law enforcement agents (e.g., those working for the FBI; Immigration and Naturalization Service (INS); Bureau of Alcohol, Tobacco, and Firearms; Drug Enforcement Agency; and other agencies). So when one reads that the CIA had not communicated with FBI agents across the country or with the INS regarding specific intelligence before September 11th, it must be understood in the context of the 1980s erection of the infamous “wall.”

Recognizing these facts, the Patriot Act changed the language of the FISA statute to require that intelligence only be a “*significant* purpose,” as opposed to primary purpose, of the FISA wiretap.²⁶ The implication of this change was that there could be other purposes for the wiretap, such as criminal prosecution. The Act further stated that those who acquire intelligence information could “consult with Federal law enforcement officers to coordinate efforts” against threats to national security.²⁷ This change sent a clear signal that the wall was henceforth eliminated. Accordingly, the Attorney General quickly issued new internal guidelines that would permit intelligence and law enforcement agents to actively share information.²⁸ However, in a unanimous opinion, the judges who comprised the standing Foreign Intelligence Surveillance Court strongly objected to these procedures and directed that the government follow steps to minimize the degree of cooperation between law enforcement agents and intelligence officials.²⁹ The DOJ then immediately appealed the orders of the

25. See *In re Sealed Case*, 310 F.3d 717, 723 (FISA Ct. Rev. 2002) (detailing the sequence of events that led to the understanding that the FISA court must inquire into the government’s purpose in seeking foreign intelligence information).

26. Patriot Act § 218, 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (emphasis added).

27. § 504, 50 U.S.C. §§ 1806, 1825.

28. Memorandum from the Office of the Attorney General on Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI (Mar. 6, 2002), <http://www.fas.org/irp/agency/doj/fisa/ag030602.html>; see also *In re Sealed Case*, 310 F.3d at 729 (explaining the Attorney General’s implementation of the Patriot Act).

29. *In re Sealed Case*, 310 F.3d at 719–21.

Foreign Intelligence Surveillance Court to a specially designated Foreign Intelligence Surveillance Court of Review.³⁰

In an opinion entitled *In re Sealed Case*,³¹ the Foreign Intelligence Surveillance Court of Review surveyed the entire history of the FISA statute and found the following:

[I]t is quite puzzling that the Justice Department, at some point during the 1980s, began to read the statute as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents. . . . [T]he definition of foreign intelligence information includes evidence of crimes such as espionage, sabotage or terrorism. . . .

The government argues persuasively that arresting and prosecuting terrorist agents of, or spies for, a foreign power may well be the best technique to prevent them from successfully continuing their terrorist or espionage activity. . . . It would seem that Congress actually anticipated the government's argument and explicitly approved it [because the definition of "agent of a foreign power" in that statute is grounded on criminal conduct^{32, 33}].

The Court thus found that the Patriot Act changed the interpretation of the FISA statute and eliminated a dichotomy that should never have been promulgated in the first place. FISA surveillance naturally has always included the possibility that intelligence-related crime might be discovered. Criminal lawyers and law enforcement agents were an integral part of effectively dealing with the national security threats posed by espionage, terrorism, and sabotage. The Criminal Division of DOJ had a natural and legally justifiable interest in receiving the information obtained via FISA surveillance. Accordingly, intelligence and law enforcement agents should be able to talk to each other without fear that their communication would somehow jeopardize obtaining a FISA warrant.

Nevertheless, the Patriot Act's change to FISA permitting the sharing with criminal investigators of intelligence information obtained solely on a finding that there was probable cause that the target was a foreign power³⁴ is the reason why the Patriot Act

30. *Id.* at 719.

31. *Id.* at 717.

32. 50 U.S.C. § 1801(b)(2)(A).

33. *In re Sealed Case*, 310 F.3d at 723–24.

34. Patriot Act § 203(a), FED. R. CRIM. P. 6(e)(3)(C); § 203(b), 50 U.S.C. §§ 2510, 2517.

was severely criticized by many for “lowering the standards” for criminal wiretaps.³⁵ This argument certainly makes sense from a theoretical standpoint. At the same time, it ignores some of the practicalities behind FISA surveillance. That is, intelligence still must be a significant purpose of the FISA wiretap so that a law enforcement agent cannot request and obtain a FISA warrant, with its technically lower standard, in a completely criminal case. Furthermore, the FISA requirements that the government prove probable cause that a target is an agent of a foreign power,³⁶ that surveillance not be based on activities protected by the First Amendment,³⁷ and that, if a United States citizen is involved, the certifications by the government not be clearly erroneous,³⁸ is hardly a cakewalk for the government. The government has stated that it can take even experienced lawyers up to a week to prepare the necessary paperwork for the FISA court, noting that the documents are “‘like mortgage applications’ in their complexity.”³⁹

In the end, it turns out that it was really not the Patriot Act that finally eliminated the wall, but the judiciary. The court in *In re Sealed Case* made it clear that it would have authorized shared use of intelligence obtained because the FISA warrant based on its interpretation of the original 1978 statute whether or not the Patriot Act had changed the language of the statute in 2001.⁴⁰ The Patriot Act apparently only provided additional support for its conclusions as to the proper utilization of intelligence surveillance.⁴¹ Accordingly, despite the controversy and allegations of reduced standards, Congress decided not to significantly change any of these FISA provisions when it passed

35. Press Release, ACLU, Surveillance under the USA Patriot Act (Feb. 7, 2003), <http://www.aclu.org/FilesPDFs/surveillance.pdf>; see also James X. Dempsey, *Civil Liberties in a Time of Crisis*, A.B.A. SEC. OF INDIVIDUAL RTS. & RESPS., HUM. RTS. MAG., Winter 2002, at 8, 10 (attacking FISA for “authoriz[ing] the FBI to conduct electronic surveillance and clandestine searches without full probable cause to believe that a crime has been or is about to be committed”).

36. 50 U.S.C. §§ 1804(a)(4)(A), 1804(a)(7)(B), 1805(a)(3)(A).

37. *Id.* § 1805(a)(3)(A).

38. *Id.* § 1805(a)(5).

39. Richard Lacayo, *Has Bush Gone Too Far?: The President’s Secret Directive to Let the NSA Snoop Without Warrants Sets Off a Furor*, TIME, Jan. 9, 2006, at 28 (internal citation omitted).

40. *In re Sealed Case*, 310 F.3d 717, 743 (FISA Ct. Rev. 2002).

41. Richard Henry Seaman and William Dylan Gardner analyze in great detail *In Re Sealed Case* in a lengthy article. Richard Henry Seaman & William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL’Y 319, 380–96 (2005).

PIRA in 2006. In fact, section 102 of PIRA made the Patriot Act permanent rather than subject to a sunset provision,⁴² and section 105 extended the deadline for renewing a FISA court order from a range of 90 to 120 days to a range of up to one year.⁴³

B. *2005–2006 Allegations of Illegal Surveillance Against al Qaeda in the United States*

It is perhaps because of the detailed requirements of the 1978 FISA statute that the Bush administration decided to investigate, without a court-ordered wiretap, al Qaeda suspects in the United States who were communicating with parties outside the country. The description of this program as domestic spying on U.S. persons, characterized by such headlines as *Time's* cover asking “Is George Bush Spying on You?,” combined with its link in the public’s mind to Patriot Act abuses, led directly to a delay of the reauthorization of the Patriot Act from December 2005 to February 2006.⁴⁴ As Senator Charles Schumer stated, “Today’s revelation that the government listened in on thousands of phone conversations without getting a warrant is shocking and has greatly influenced my vote. . . . Today’s revelation makes it clear we have to be very careful—very careful.”⁴⁵ Former Congressman Bob Barr spoke for many government critics when he wrote:

The Supreme Court has unanimously rejected the assertion that a President may conduct electronic surveillance without judicial approval for national security, noting in 1972 [in *United States v. U.S. District Court*⁴⁶] that our “Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch.” Rather than abiding such a clear missive, the Administration instead is taking the road mapped out nearly two centuries ago by Andrew Jackson,

42. Patriot Act § 224, *repealed by* PIRA § 102.

43. PIRA § 105, 50 U.S.C. § 1805(e)(2).

44. See *Patriot Act Renewal Fails in Senate: GOP Fights to Save Provisions Before End-of-Year Deadline*, *supra* note 2.

45. *Id.*

46. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 316–17 (1972).

who, in response to a Supreme Court decision he didn't like, ignored it⁴⁷

How exactly did the administration come to the conclusion that it could conduct electronic surveillance of al Qaeda suspects in the United States involved in international communications without obtaining a FISA warrant? A review of the written justification submitted to Congress by the Department of Justice on December 22, 2005,⁴⁸ and Attorney General Alberto Gonzales' later public statements⁴⁹ indicates that this decision was based completely on pre-Patriot Act precedents. Specifically, the Supreme Court's opinion in *United States v. United States District Court*, quoted only in part by Representative Barr above, included language narrowing the decision to cases involving purely domestic threats (in that case, anti-war protesters who burned an ROTC building). The court noted that the executive had routinely conducted electronic surveillance without a warrant when confronting foreign-based national security threats and stated, "We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."⁵⁰ The Foreign Intelligence Court of Review had also noted that "all the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. . . . We take for granted that the President does have that authority."⁵¹

Critics argued, however, that the original 1978 FISA statute (which had gone beyond anything required in the 1972 Supreme Court decision in *United States v. United States District Court*) explicitly stated that the president must obtain a court order before conducting any surveillance of a U.S. person in the

47. Bob Barr, *Presidential Snooping Damages the Nation: Bush Has Put Himself Above the Law and in the Company of Rogues*, TIME, Jan. 9, 2006, at 34.

48. Letter from U.S. Dep't of Justice Assistant Att'y Gen. William E. Moschella to Senators Pat Roberts and John Rockefeller and Congresspersons Peter Hoekstra and Jane Harman (Dec. 22, 2005), <http://www.usdoj.gov/ag/readingroom/surveillance6.pdf>.

49. Alberto R. Gonzales, Op-Ed., *America Expects Surveillance*, WALL ST. J., Feb. 6, 2006, at A18; see also Katherine Shrader, *Senators Question Gonzales on NSA Wiretaps*, BOSTON.COM, Feb. 6, 2006, http://www.boston.com/news/nation/washington/articles/2006/02/06/gonzales_calls_nsa_eavesdropping_lawful/ (summarizing Attorney General Alberto Gonzales' testimony before the Senate Judiciary Committee).

50. *Keith*, 407 U.S. at 321–22.

51. *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002).

United States even if the communication was international and involved agents of a foreign power.⁵² The Department of Justice responded that FISA could be overridden by later statutes and the Congressional Authorization for the Use of Military Force (AUMF)⁵³ passed in 2001 was such a statute. As interpreted by the Supreme Court in *Hamdi v. Rumsfeld*, the AUMF authorized the president to utilize all “fundamental and accepted . . . incident[s] to war.”⁵⁴ Therefore, as “[c]ommunications intelligence targeted at the enemy is a fundamental incident of the use of military force,”⁵⁵ the warrantless surveillance was proper.⁵⁶

Only the Supreme Court can resolve this matter. One of the questions the Court would have to answer is whether, in light of Congress’ action, *Youngstown Sheet & Tube Co. v. Sawyer*⁵⁷ requires the nullification of any pretense of inherent executive authority. There is the further question of whether President Jimmy Carter’s signing of FISA in 1978 might have waived any future claim of presidential power. On the other hand, Senator Pat Roberts has argued that “Congress, by statute, cannot extinguish a core constitutional authority of the President.”⁵⁸ His statement is reinforced by the Foreign Intelligence Court of Review’s opinion that “FISA could not encroach on the President’s constitutional power.”⁵⁹ Fortunately, there may be cases in which defendants have standing to force the courts to accept jurisdiction. For example, “government officials have been telling reporters that the disputed NSA wiretaps played a part in building the case that led to guilty pleas by two plotters”: Lyman Farris, who intended to destroy the Brooklyn Bridge, and Mohammed Junaid Babar, who smuggled money to al Qaeda.⁶⁰ In the future, however, the DOJ has indicated it will obtain approval from the FISA court utilizing new procedures it hopes

52. 50 U.S.C. § 1805 (1998).

53. S.J. Res. 23, 107th Cong., 115 Stat. 224 (2001).

54. 542 U.S. 507, 518 (2004).

55. Letter from U.S. Dep’t of Justice Assistant Att’y Gen. William E. Moschella, *supra* note 48, at 3.

56. *Hamdi*, 542 U.S. at 509.

57. 343 U.S. 579 (1952).

58. *Senate Intelligence Chairman: Bush Can Spy*, KNOWLEDGEDRIVENREVOLUTION.COM, http://www.knowledgedrivenrevolution.com/Articles/200602/20060206_Bush_Can_Spy.htm (last visited May 2, 2007).

59. *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002).

60. Lacayo, *supra* note 39, at 32.

will not interfere with the government's need to ensure speed and agility in intercepting al Qaeda communications.⁶¹

Regardless of the eventual outcome of this dispute, however, the NSA surveillance question is characteristic of the controversy surrounding the Patriot Act. Specifically, sound bites are completely incapable of explaining the issues, and the government's action in many cases is more a reflection of previously unknown prior law than anything that is completely novel or created without logical foundation. At the same time the furor surrounding the matter directly influenced the public's perception of the Patriot Act and Congress's attitude towards reauthorization of its existing provisions.

C. From Law Enforcement to Intelligence

Prior to passage of the Patriot Act, prosecutors or FBI agents who came across significant intelligence information while utilizing procedures common to criminal investigations had no legal mechanism for sharing this information with the intelligence community.⁶² Specifically, if they uncovered evidence of espionage or a terrorist plot or the identity and locations of spies and terrorists during the course of interrogating a witness before a grand jury, reviewing records subpoenaed by the grand jury, or monitoring a wiretap, they could not legally share this information with the CIA. In addition, an FBI agent or police officer who accessed a criminal history check on a foreign visa applicant was not allowed to pass this information on to the Department of State officer who would determine whether the applicant entered or reentered the country. This forced lack of communication was a product of statutes pertaining to information obtained during a grand jury investigation,⁶³ Title III criminal wiretaps,⁶⁴ and reviews of records maintained in the computerized national criminal history information data bank.⁶⁵ These statutes and rules of criminal procedure were crafted so that this type of information

61. Letter from Attorney General Alberto R. Gonzales to Senators Patrick Leahy and Arlen Specter (Jan. 17, 2007), <http://leahy.senate.gov/press/200701/011707a.htm> (follow "PDF letter from Department of Justice" hyperlink).

62. *See infra* notes 62–64 and accompanying text.

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

64. 18 U.S.C. § 2517 (1998).

65. 28 U.S.C. § 1534(d), (e).

would be utilized only by law enforcement officials, not intelligence officials.

In his testimony before the United States Senate Judiciary Committee, U.S. Attorney Fitzgerald also described the effect of such statutes in relation to an attempt to locate an individual named “Harun” who was responsible for the bombing of the U.S. embassy in Nairobi, Kenya. Wadi el Hage, a bin Laden confidant, had testified briefly before the grand jury in New York and had specifically mentioned “Harun.” During el Hage’s testimony:

El Hage chose to lie repeatedly . . . , but even in his lies he provided some information of potential use to the intelligence community—including potential leads as to the location of his confederate Harun and Harun’s files in Kenya. Unfortunately, as el Hage left the grand jury room . . . we also knew that we would not be permitted to share the grand jury information with the intelligence community.⁶⁶

In this instance, Fitzgerald found a way around the restrictions of Federal Rule of Criminal Procedure 6(e) by persuading el Hage to answer the questions of an agent outside the grand jury room. But, as he noted, “In essence, we solved the problem only by obtaining the consent of a since convicted terrorist. We do not want to have to rely on the consent of al Qaeda terrorists to address the gaps in our national security.”⁶⁷

Section 203 of the Patriot Act amended Rule 6(e) by adding subsection (3)(D), which authorizes the sharing of “foreign intelligence, counterintelligence, . . . [and] foreign intelligence information” obtained in the grand jury process with “intelligence, national defense, or national security official[s] to assist . . . in the performance of [their official] duties.”⁶⁸ Also, the Patriot Act and the Homeland Security Act of 2002 amended FISA to permit the disclosure to counter-terrorism and intelligence officials of relevant information obtained during a criminal wiretap.⁶⁹ And further, the Patriot Act provides that

66. *Hearing on Protecting Our National Security from Terrorist Attacks: A Review of Criminal Terrorism Investigations and Prosecutions Before the S. Comm. on the Judiciary*, *supra* note 19, at 5.

67. *Id.*

68. Patriot Act § 203(a), FED. R. CRIM. P. 6(e)(3)(C).

69. Patriot Act § 203(b)(1), 18 U.S.C. § 2517(6); Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002) (codified in scattered sections of 3, 5, 6, 7, 8, 10, 18, 26, 28, 31, 40, 41, 42, 49, and 50 U.S.C.).

when the INS and Department of State examine and adjudicate visas, they can access information contained in the national criminal history computer as to an applicant's arrests and convictions.⁷⁰

Public criticism of the new procedures involving the transfer of information from law enforcement to intelligence agencies has been, for the most part, muted, especially compared to the other provisions reviewed in this article. There have been general concerns about the sharing and accumulation of information,⁷¹ and some have expressed fears that the intelligence communities might “erode the rights of American citizens” that have been established in our system of criminal justice,⁷² but nothing specific has excited the media or stirred the masses. Academics, however, have focused in on theoretical threats to traditional principles of grand jury secrecy as well as the proper use of the grand jury. Sara Sun Beale and James E. Felman acknowledge that two of the purposes of grand jury secrecy, protecting the identity of witnesses and ensuring that targets will not flee before the investigation is complete, are unlikely to be compromised by the Patriot Act provisions permitting the disclosure of information to intelligence agencies.⁷³ But they note that intelligence agencies may be less attuned than federal prosecutors to the third purpose, which they identify as protecting the reputation of those implicated by grand jury information.⁷⁴ Furthermore, in their opinion, the broad definition of “foreign intelligence and counterintelligence information” could lead to a “backdoor expansion” of the power of the grand jury, bolstered by the threat of contempt, “to compel witnesses to disclose information and documents regarding the diplomatic strategies of other countries [even on] issues relat[ing] solely to trade or economic concerns”⁷⁵

70. Patriot Act § 403, 8 U.S.C. § 1105.

71. Podesta, *supra* note 16.

72. See Sara Sun Beale & James E. Felman, *Assessing the USA PATRIOT Act's Changes to Grand Jury Secrecy*, A.B.A. CRIM. JUST. SEC., CRIM. JUST. MAG., Summer 2002, <http://www.abanet.org/crimjust/cjmag/17-2/patriot.html> (referencing William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U.L. REV. 1 (2000)).

73. *Id.*

74. *Id.*

75. *Id.*

Beale and Felman admit that in many instances there may be a clear need for disclosure of grand jury information to the intelligence community.⁷⁶ To meet this need and protect against the dangers they contemplate, they have recommended that the Patriot Act be amended to require a court to approve in advance any disclosure of information to intelligence agencies.⁷⁷ Sara Levy, in her article on the Patriot Act and the grand jury exception, also argues for more judicial supervision prior to disclosure.⁷⁸

These proposals on their face do not appear to be objectionable. Rule 6(e) already demands that the court approve in advance any disclosure of federal grand jury information to state law enforcement agencies for use in state prosecutions.⁷⁹ But, as Beale and Felman acknowledge, the reputation of a target is just as likely to be affected by the leaks of witnesses, who are not held to secrecy by federal grand jury rules, as it is by revelations from members of the intelligence community, who are legally prohibited from unauthorized disclosure.⁸⁰ Intelligence agencies may not always think like criminal prosecutors, but when it comes to maintaining secrecy they are of the same mind. As for concerns that the ability to share foreign intelligence and counter-intelligence information may lead to an expansion of the role of the criminal grand jury, aside from the fact that most of this information involves the federal crimes of terrorism and espionage, it must be noted that the Patriot Act still requires that the government advise the court afterwards of the “information . . . disclosed and the departments, agencies, or entities to which the disclosure was made.”⁸¹ Any attempt to use the grand jury simply for issues of foreign policy, therefore, in addition to being unethical, should be quickly shut down by the court.

Congress has apparently not been influenced by the arguments for prior court approval of disclosure, as PIRA contained no reference to changing the original Patriot Act rules on grand juries. It is nevertheless still possible that

76. *Id.*

77. *Id.*

78. Sara Levy, *The Patriot Act Grand Jury Disclosure Exception: A Proposal for Reconciling Civil Liberty and Law Enforcement Concerns*, 5 CHI. KENT J. INT'L & COMP. L. 2, 27 (2005).

79. FED. R. CRIM. P. 6(e)(3)(C).

80. Beale & Felman, *supra* note 72, at 6; FED. R. CRIM. P. 6(e)(3)(D)(i).

81. FED. R. CRIM. P. 6(e)(3)(D)(ii).

Congress may respond to the dispute at a later date, as the original House of Representatives version of the Patriot Act did contain a requirement for prior approval.⁸² The complaints about the absence of such provisions, however, have still been more academic than public.

III. WELCOME TO THE TWENTY-FIRST CENTURY: PROVIDING COMPUTER RECORDS TO INTELLIGENCE AND LAW ENFORCEMENT OFFICIALS

The author has attended numerous seminars, conferences, and meetings where the speakers made passionate claims along the lines that the Patriot Act permits the government to access someone's computer and read their e-mails without a warrant.⁸³ The *New Republic* suggested that the Patriot Act gave the government "essentially unlimited authority to install recording devices to monitor" Internet use.⁸⁴ The ACLU web site states that under the Patriot Act "the FBI can secretly conduct a physical search or wiretap . . . to obtain evidence of crime without proving probable cause . . ."⁸⁵ These proclamations, although understandable in light of the general public descriptions of the Patriot Act referenced earlier, do not appear to be an accurate reflection of the actual legislation.

There is no question that the Patriot Act recognized that society communicates today via the Internet the way we formerly communicated by the telephone. Those of us who chastised our children for talking too much on the telephone on school nights now find that, while typing a paper on the home computer, they are simultaneously communicating with five of their friends on an instant messenger program. Welcome to the twenty-first century.

A. *Computer Contact Information*

The Patriot Act attempted to catch up with today's technology in part by authorizing the rough equivalent of telephone "pen registers" on e-mail and Internet communication. In other words, when the government is conducting an investigation and

82. H.R. REP. NO. 107-236, at 30 (2001).

83. Patriot Act Conferences & Meetings, *supra* note 10.

84. Jeffrey Rosen, *Tapped Out: The Terrorism Bill Does Too Much and Not Enough*, THE NEW REPUBLIC, Oct. 15, 2001, at 12.

85. Press Release, Surveillance under the USA Patriot Act, *supra* note 35.

suspects a potential criminal is using a phone to contact others of like mind, the law permits an agent or prosecutor to obtain a court order from a judge directing the phone company to place a pen register/trap-and-trace device on the defendant's phone.⁸⁶ To obtain the order the government must certify that the information sought is "relevant to an ongoing [federal] criminal investigation."⁸⁷ These pen requests and trap-and-trace devices do *not* record the content of the call; rather, they provide a list of phone numbers of calls both dialed and received by the suspect.

Interestingly, there apparently has never been an explicit constitutional requirement to obtain such court orders. The Supreme Court held in 1979 in *Smith v. Maryland* that there was no legitimate expectation of privacy and thus no Fourth Amendment interest in the numbers one dials or the ownership of that list because this information is voluntarily shared with the phone company.⁸⁸ It made no difference that the information was being recorded and maintained in an automated system as opposed to being communicated to a human telephone operator, as this was just a more efficient way for the third party to do business and obtain access when necessary.⁸⁹ The Court's decision was consistent with its ruling just three years before that there was no Fourth Amendment interest in the prevention of government access to bank records because the information was conveyed to a third party.⁹⁰

Many arguments may eventually be made challenging the holding of *Smith* and its applicability to communications in the twenty-first century. Specifically, society may be prepared to recognize a legitimate expectation of privacy in this information today when it was not prepared to do so in 1979 on the heels of what had been the routine assistance of the live operator. In addition, Internet addresses may be more sensitive than numbers dialed, and computer communications may be more secure and private than telephone conversations ever have been. Regardless, *Smith* has yet to be overruled by the Supreme Court.

86. 18 U.S.C. §§ 3121–3127 (2006).

87. *Id.* § 3122(b).

88. 442 U.S. 735, 742 (1979).

89. *Id.* at 745.

90. *United States v. Miller*, 425 U.S. 435, 442–43 (1976).

Concerned about the wide open access to communications suggested by the Supreme Court's decision in *Smith*, Congress, at the telecommunications industry's behest, reacted by passing the Electronic Communications Privacy Act of 1986.⁹¹ The Act mandated, as noted above, that the government must obtain a court order based on a certification that the information is relevant to a federal criminal investigation before it can obtain telephone pen register and trap-and-trace information.⁹²

Of course today, with everybody, including terrorists and spies, using the Internet instead of the telephone to communicate, a summary of telephone numbers may not help either criminal or intelligence investigations, but a review of e-mail addresses a suspect has been in communication with could prove invaluable. As the information the government might seek pertaining to computer communications is very similar, if not exactly the same, as that obtained with a pen register and trap-and-trace device (in other words, both kinds of lists compile non-content-based data indicating which e-mail addresses are in contact with each other), the Patriot Act applied essentially the same Electronic Communications Privacy Act standards and procedures to obtain a printout of Internet contacts. The government must secure an order from a court after articulating facts that demonstrate the information is "relevant to an ongoing criminal investigation"⁹³ or "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."⁹⁴ The debate over these provisions can best be understood after an explanation of their use in conjunction with national security letters, a separate tool which has spawned its own controversy.

B. *National Security Letters*

The information the government receives from a pen register-like device on a telephone or computer may simply be a list of

91. Pub. L. No. 99-508, § 201, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C.).

92. 18 U.S.C. § 3122(b) (2006).

93. Patriot Act § 216, 18 U.S.C. § 3123(a).

94. § 214, 50 U.S.C. § 1842(c)(2); *see also* § 216(a)(2), 18 U.S.C. §§ 3123(b)(1) (adding the words "or other facility" in reference to what the pen register or trap-and-trace device may be attached or applied to), 3127(3), (4) (adding the term "routing information" to the definition of "pen register" so as to accommodate Internet communication).

phone numbers or e-mail addresses like T-man@yahoo.com or B-man@earthlink.net. The government still has no idea who exactly made or uses these e-mail addresses unless it obtains identifying data indicating to whom the account is assigned or who pays to maintain the e-mail address. In the criminal context this information has long been obtained by administrative subpoenas, while in the intelligence context the FBI has utilized national security letters (NSLs). The statutory provision setting forth the procedure for using NSLs specifically prohibits the recipients of such letters from disclosing that the FBI has sought access to the records.⁹⁵

The Patriot Act expanded this provision slightly by dropping the requirement that the subject of the investigation must be an agent of a foreign power; it is now proper to utilize an NSL in cases where the information is relevant to an investigation of terrorism or clandestine intelligence activity.⁹⁶ Additionally, the Fair Credit Reporting Act was amended to allow the FBI to use NSLs to obtain credit reports.⁹⁷

The tremendous increase in terrorism investigations after September 11th led to a corresponding increase in the number of NSLs issued.⁹⁸ Revelation of this fact, combined with the media's description of the letters and the atmosphere surrounding anything linked with the Patriot Act, led to great public sensitivity about their use.⁹⁹ The *Washington Post* noted that "the letters—one of which can be used to sweep up the records of many people—are extending the bureau's reach as never before into the telephone calls [and] correspondence . . . of ordinary Americans."¹⁰⁰ An NPR source stated, "[NSLs] are issued secretly under the Patriot Act with no judicial oversight. They require Americans to cough up loads of information on colleagues and clients—maybe you—and to never breathe a word to anyone of what they've done."¹⁰¹ In addition, a March 2007 report by the Department of Justice

95. 18 U.S.C. § 2709(c)(1).

96. Patriot Act § 505(a), 18 U.S.C. § 2709(b).

97. § 358(g), 15 U.S.C. § 1681(v).

98. Barton Gellman, *The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, WASH. POST, Nov. 6, 2005, at A01.

99. *Id.*

100. *Id.*

101. TOM ASHBROOK, *National Security Letters: Use or Misuse?*, on ON POINT (Nat'l Pub. Radio 2005), available at http://www.onpointradio.org/shows/2005/11/20051110_a_main.asp.

Inspector General highlighting technical mistakes in the issuance of NSLs¹⁰² was quickly characterized as FBI abuse of the process.¹⁰³

This kind of language of course played to the fears of listeners and readers, although the actual use of the letters and the information obtained would not appear to be quite so sinister. NSLs are fairly limited and targeted at information that an individual has not kept private but shared with third parties.¹⁰⁴ The Inspector General's report clearly indicated that there was no improper use of the letters against individuals who were not legitimate suspects and that there were no deliberate violations of federal law, but rather poor recordkeeping and sloppy bureaucratic procedures. For instance, the report noted that a study of the issuance of NSLs "did not reveal deliberate or intentional violations of NSL statutes" and, in one section, that "[a]lthough the majority of the possible violations—22 of 26—arose from FBI errors, most of them occurred because of typographical errors or the case agent's good faith but erroneous belief that the information related to [a formally approved] investigative subject."¹⁰⁵

Regardless, NSL recipients were now on notice that the letters might somehow be improper and for the first time in the long history of the utilization of NSLs, the government was repeatedly challenged by NSL recipients in court.¹⁰⁶ The lower courts were not unsympathetic to the complaints they received. In *Doe v. Ashcroft*, the District Court questioned the use of NSLs because, unlike grand jury and administrative subpoenas, which are at least subject to theoretical judicial oversight when they are challenged, there is no established mechanism for the recipient of an NSL to appeal compliance to the courts.¹⁰⁷ Furthermore, in the court's opinion, the nondisclosure provisions violated the

102. U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (March 2007), available at <http://fas.org/irp/agency/doj/oig/natsec> [hereinafter OIG REPORT].

103. Press Release, Patrick Leahy, U.S. Sen., Reaction Of Sen. Patrick Leahy, Chairman, Senate Judiciary Committee, On The Inspector General's Report On The Use Of National Security Letters (Mar. 9, 2007), available at <http://leahy.senate.gov/press/200703/030907.html>.

104. See, e.g., *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

105. OIG REPORT, *supra* note 102, at xxx.

106. See, e.g., *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004); *Doe v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005).

107. 334 F. Supp. 2d 471, 475, 494–511 (S.D.N.Y. 2004).

First Amendment because the recipient could not cite the letter or the fact that it was received in furtherance of the public debate or for historical purposes even long after the potential danger from the targeted terrorist attenuated.¹⁰⁸ The recipient technically could not even provide the letter to an attorney to file a complaint if the recipient so desired.¹⁰⁹ The District Court in *Doe v. Gonzales* characterized the nondisclosure provisions as a prior restraint on substantive speech:

Considering the current national interest in and the important issues surrounding the debate on renewal of the PATRIOT Act provisions, it is apparent to this court that the loss of Doe's ability to speak out now on the subject as a NSL recipient is a real and present loss of its First Amendment right to free speech that cannot be remedied. Doe's speech would be made more powerful by its ability to put a "face" on the service of the NSL, and Doe's political expression is restricted without that ability. . . . Doe's statements as a known recipient of a NSL would have a different impact on the public debate than the same statements by a speaker who is not identified as a recipient.¹¹⁰

In what sometimes appeared to be an over-anxious effort to proclaim that a court has found substantial sections of the Patriot Act unconstitutional (when, to date, no appellate court has made such a finding), the *Washington Post* headlined "Key Part of the Patriot Act Ruled Unconstitutional: Internet Providers' Data at Issue" after the lower court's ruling in *Doe v. Ashcroft*.¹¹¹ The *New York Times* bannered that "Judge Strikes Down Section of Patriot Act Allowing Secret Subpoenas of Internet Data."¹¹² There was the same reaction when the Ninth Circuit vacated part of the Clinton-era "'material support' to terrorism" provision, resulting in the public being informed that "Judge's Ruling Indicates Part of PATRIOT Act Is Unconstitutional."¹¹³ The reality in all three cases was that the

108. *Id.* at 475.

109. *Id.* at 496.

110. 386 F. Supp. 2d 66, 72-73 (D. Conn. 2005).

111. Don Eggen, *Key Part of Patriot Act Ruled Unconstitutional: Internet Providers' Data at Issue*, WASH. POST, Sept. 30, 2004, at A16.

112. Julia Preston, *Judge Strikes Down Section of Patriot Act Allowing Secret Subpoenas of Internet Data*, N.Y. TIMES, Sept. 30, 2004, at A26.

113. *Judge's Ruling Indicates Part of PATRIOT Act Is Unconstitutional*, BALTIMORE CHRON. & SENTINEL, July 3, 2002, available at http://www.baltimorechronicle.com/patriotact_jul02.shtml.

courts' decisions were primarily targeted at preexisting law that had only been slightly modified by the Patriot Act. The courts did not specifically object to the Patriot Act additions to FISA. To their credit, the *New York Times* and *Washington Post* published later corrections, noting that, “[w]hile the Patriot Act loosened restrictions on the use of the letters, most of U.S. District Judge Victor Marrero’s ruling focused on earlier statutes governing the letters,”¹¹⁴ and that the statute in question, enacted in 1986, “was not created” under the Patriot Act.¹¹⁵

The government objected to the lower courts’ findings that NSLs required judicial supervision and that nondisclosure provisions violated the First Amendment. *Smith* had already indicated there was no Fourth Amendment interest or legitimate expectation of privacy in information shared with the phone company.¹¹⁶ As a practical matter, as the Court in *Ashcroft* acknowledged, there is virtually no judicial supervision of grand jury and administrative subpoenas except in the rare instances they are contested.¹¹⁷ Furthermore, the First Amendment is not absolute.¹¹⁸ The disclosure of the receipt of an NSL directed at a terrorist target would strike a law enforcement official more as obstruction of justice or a direct threat to national security than as enlightening public discourse. In fact, Congress had years before enacted statutes that prohibited the disclosure of financial subpoenas¹¹⁹ and electronic wiretaps¹²⁰ and these have never been challenged in court.¹²¹

114. Don Eggen, *Key Part of Patriot Act Ruled Unconstitutional: Internet Providers’ Data at Issue*, correction, WASH. POST, Oct. 1, 2004, at A16.

115. Julia Preston, *Judge Strikes Down Section of Patriot Act Allowing Secret Subpoenas of Internet Data*, correction, N.Y. TIMES, Oct. 1, 2004, at A26 (“An article yesterday about a judge’s ruling to invalidate some federal surveillance powers referred incorrectly to a subpoena statute that was struck down. While the statute . . . was amended by . . . the USA Patriot Act, it was not created under that act. . . . The judge’s ruling analyzed and struck down the statute as a whole, including provisions that predated the Patriot Act.”).

116. *Smith v. Maryland*, 442 U.S. 735, 744–45 (1979).

117. *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 484–86 (S.D.N.Y. 2004).

118. *See United States v. O’Brien*, 391 U.S. 367, 376 (1968) (“We cannot accept the view that an apparently limitless variety of conduct can be labeled speech whenever the person . . . intends thereby to express an idea.”).

119. *See* 18 U.S.C. § 1510(b)(1) (2006) (imposing fines or imprisonment on anyone disclosing the existence or contents of a subpoena for records maintained by a financial institution).

120. *See id.* § 2511(2)(a)(ii) (mandating that it is unlawful for anyone to disclose the existence of electronic surveillance).

121. The author has reviewed the annotations and found no case where these nondisclosure provisions were challenged.

Accordingly, the DOJ appealed the decisions in *Doe v. Ashcroft* and *Doe v. Gonzales*. These appeals were consolidated at the Second Circuit Court of Appeals.¹²² At the same time, the government opposed any attempt to modify the requirements of NSLs during the Patriot Act renewal debate in Congress. Congress agreed that there was no requirement for prior judicial oversight of NSLs, but was concerned that recipients could not consult a lawyer or seek judicial intervention if they questioned compliance.¹²³ Congress also accepted the argument that it made no sense for the statute to be worded so as to require permanent nondisclosure in perpetuity.¹²⁴ PIRA thus provided that NSL recipients could consult with a lawyer and that nondisclosure would be limited to situations where the FBI certified that disclosure would endanger an individual or national security or interfere with an ongoing investigation. The recipient can also challenge nondisclosure orders in court and petition the court for review of an adverse ruling after one year upon a claim of changed circumstances.¹²⁵

Based on PIRA's provisions permitting judicial review,¹²⁶ the Second Circuit declared moot any Fourth Amendment challenges to providing the data requested by NSLs.¹²⁷ It left open the question of whether the recipients' First Amendment rights had been violated, noting that PIRA now provided a mechanism for the recipients to further litigate that question in each individual case at the district court level.¹²⁸

C. Content

As noted earlier, the pen register devices applied to computers are designed to record addresses, not content. In fact, FISA mandates that the government avoid collection of content when tracing devices are utilized.¹²⁹

122. *Doe I v. Gonzales*, 449 F.3d 415 (2d Cir. 2006).

123. *See, e.g.*, 50 U.S.C. § 1861(d)(1)(B) (allowing the recipient of an NSL to consult an attorney to obtain legal advice regarding the letter).

124. *See, e.g., id.* § 1861(f)(2)(C)(i) (allowing disclosure unless judge finds a reason to believe that disclosure would endanger national security or interfere with an investigation).

125. PIRA § 115, 18 U.S.C. § 3511.

126. § 507(c), 28 U.S.C. § 2265.

127. *Doe I v. Gonzales*, 449 F.3d 415, 419 (2d Cir. 2006).

128. *Id.*

129. 18 U.S.C. § 3121(c).

The ACLU, however, claimed that these “addresses are rich and revealing content” in themselves because they are more “than a simple list of the people we have communicated with; it is intimate information that reveals who we are and what we are thinking about—much more like the content of a phone call than the number dialed.”¹³⁰ There does appear, on the surface, to be some merit to this argument. As technically explained by Peter Madrinan in his article on the Internet surveillance provisions of the Patriot Act:

As a result of the fungible characteristics of Internet addresses—in the numeric form of an IP address or the symbolic form of a URL—the manner in which computers communicate is dissimilar to communications taking place over the telephone. When a person makes a telephone call, the substance of the call itself—the contents of the communication—are separable and “evanescent” from the transactional data utilized to make the connection. In other words, an investigator cannot re-dial the telephone number captured by a pen/trap device and listen to a conversation that took place in the past. But, when a PATRIOT’s pen/trap device merely captures the data sent or received by a targeted computer, the information exchanged between computers exhibits nearly genetic qualities: by re-entering the recorded string of information such as a URL into a web browser, an investigator can recreate with high levels of assurance, exactly what was displayed on the targeted computer.¹³¹

Madrinan goes on to explain that with a pen register device the FBI could thus determine whether the suspect utilized Google, then contacted a website on crop dusters and pesticides, and from there checked another website on professional pest control products from Italy.

But, on reflection, one realizes that traditional pre-Patriot Act pen registers accompanied by subscriber information obtained through administrative subpoenas and NSLs have also routinely revealed more than simply the numbers dialed. If the target called the Islamic Association for Violence in the Middle East, the pen register and subscriber data obtained would reveal this information just as much as if an individual visited a web address

130. ACLU.org, Surveillance under the USA PATRIOT Act, Apr. 3, 2003, <http://www.aclu.org/safefree/general/17326res20030403.html>.

131. Peter Madrinan, *Devil in the Details: Constitutional Problems Inherent in the Internet Surveillance Provisions of the USA PATRIOT Act of 2001*, 64 U. PITT. L. REV. 783, 806 (2003).

entitled “Islamic Association for Violence in the Middle East.” Furthermore, if a physical location or web site is open to all and the target can access it freely, the government could do so also. It is unclear, therefore, how the government would necessarily be obtaining any more private content with a computer pen register device than it obtains by tracking the numbers and addresses with a telephone pen register device.

To date there have been no significant cases overturning the above provisions on the basis that they impermissibly access content. PIRA also did not make any major changes in these provisions, amending the provision mandating that the government avoid gathering content simply by adding the necessary terms to apply FISA to Internet communications.¹³²

The Patriot Act did not in any way change the standard that has traditionally been applied when the government is seeking the substance of communications as opposed to just a listing of who is talking to whom. Specifically, to record the content of substantive communication in a criminal case, the law still requires that the government show the court probable cause that the suspect is attempting to further criminal activity.¹³³ The Patriot Act simply added terrorism-related crimes, such as drug trafficking, bank fraud, money laundering, and gambling, to the laundry list of offenses to which the standards for intercepting communications have always applied.¹³⁴ To obtain content in an investigation that has a significant intelligence purpose, the government must still show probable cause that the suspect is acting as an agent of a foreign power.¹³⁵

As indicated in the earlier section discussing FISA wiretaps, court orders to obtain wire or computer taps based on probable cause are lengthy—“like mortgage applications’ in their complexity.”¹³⁶ Unlike what may be depicted on television and in movies, Chief Investigator McGarrett does not generally turn to his assistant, say “Danno get a wiretap,” and twenty-four hours later sit in a van outside a residence monitoring phone calls or conversations held inside someone’s living room. The showing of probable cause routinely entails drafting a lengthy affidavit

132. Patriot Act § 216, 18 U.S.C. § 3121(c).

133. 18 U.S.C. § 2518(3)(a).

134. *See id.* § 2516.

135. 50 U.S.C. § 1805(a)(3)(A).

136. Lacayo, *supra* note 39, at 28.

containing solid information demonstrating to any objective party that probable cause exists. The affidavit and accompanying technical paperwork has to be reviewed and approved by separate legal offices at the FBI and DOJ and then officially authorized by a very high ranking DOJ official. It is only after that review that the attorney and agent bring the affidavit and paperwork to a neutral United States district judge to request authorization to begin the interception.¹³⁷

IV. “SNEAK AND PEEK” WARRANTS

Section 213 of the Patriot Act authorized so-called “sneak and peak” warrants.¹³⁸ As mentioned above, at numerous ACLU meetings representatives stated in effect that “sneak and peak” warrants now permit the government to search someone’s home without a warrant or showing of probable cause, then report back to the court only if evidence is found.¹³⁹ The ACLU made this claim:

For centuries, common law has required that the government can’t go into your property without telling you, and must therefore give you notice before it executes a search. That “knock and announce” principle has long been recognized as part of the Fourth Amendment of the Constitution.

The Patriot Act, however, unconstitutionally amends the Federal Rules of Criminal Procedure to allow the government to conduct searches without notifying the subjects, at least until long after the search has been executed.¹⁴⁰

The above assertions are inaccurate and demonstrate a misunderstanding of prior law as well as the Patriot Act. If pursuant to a warrant the government conducts a search of one’s home when he or she is not present, agents must leave behind a “notice” of entry summarizing what has been found.¹⁴¹ This procedure works fine in the vast majority of drug trafficking, bank fraud, and other cases handled by federal

137. See 18 U.S.C. §§ 2516–2519 (more specifically, section 2518); 50 U.S.C. §§ 1821–1829 (more specifically, sections 1823–1824).

138. 18 U.S.C. § 3103(a).

139. Patriot Act Conferences & Meetings, *supra* note 10.

140. ACLU.org, Surveillance under the “USA/Patriot” Act, Jan. 1, 2002, <http://www.aclu.org/privacy/spying/14889prs20020101.html>.

141. See Patriot Act § 213, 18 U.S.C. § 3103a(b) (“any notice required, or that may be required, to be given may be delayed if [certain requirements are met]”).

agents. Occasionally, however, it is necessary to conduct a search or enter a home without leaving notice behind, such as in cases where notice would compromise the investigation. For example, it would not make sense for the government to enter the office of the head of the New Orleans Mafia and plant a bug above his desk if it were then required to leave a notice on his door that agents had been there. In the electronic surveillance context, the search might be a wiretap or a surreptitious entry to plant a listening device. In those situations, federal law has long provided that notice may be delayed by court order until the court believes that notice may be provided without compromising the investigation.¹⁴²

The same legal principle also has long applied to routine home or office searches where it is clear that providing immediate notice will endanger informants, lead to the destruction of evidence, or seriously undermine an ongoing investigation.¹⁴³ As the Court stated in *United States v. Villegas*, “[c]ertain types of searches and surveillance depend for their success on the absence of premature disclosure. . . . When nondisclosure of the authorized search is essential to its success, neither [Federal] Rule [of Criminal Procedure] 41 nor the Fourth Amendment prohibits covert entry.”¹⁴⁴ The Supreme Court has also stated in *Dalia v. United States* that contentions that searches are unconstitutional for lack of notice are frivolous.¹⁴⁵

Because this common sense procedure has been embodied in written court decisions but not explicitly set forth in legislation, the mechanism for necessary delay was always subject to how a particular circuit court of appeals might interpret the case law. The Patriot Act provided a statutory basis for the delayed notice, ensuring uniform application of the principle. Pursuant to the statute, if the government shows a court reasonable cause to believe that immediate notice of a routine government search of a home, office, or other premises may have an adverse result, such as the endangerment of the life or physical safety of an individual, flight from prosecution, destruction of or tampering

142. 18 U.S.C. § 2518(8)(d).

143. *See, e.g.*, *United States v. Villegas*, 899 F.2d 1324 (2d Cir. 1990); *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986).

144. *Villegas*, 899 F.2d at 1336.

145. 441 US 238, 247 (1979).

with the evidence, or seriously jeopardizing an investigation, the court may delay notice for a reasonable time determined by the court.¹⁴⁶ All requests for extensions must be approved by the judge and notice still must be provided at some time after the execution of the warrant.¹⁴⁷ This procedure of delayed notice is all that the now infamous “sneak and peak” provisions of the Patriot Act authorize. There is nothing that permits a search without a warrant or without probable cause.

The complaint of Patriot Act critics that the government can conduct a search and never give notice of that search did have some basis in that the Patriot Act, while permitting the court to delay notice for a reasonable time, did not specify a clear time limit.¹⁴⁸ The electronic surveillance statutory precedent for the concept of delayed notice mandated that notice be delayed only up to ninety days unless the court granted an extension for good cause.¹⁴⁹ PIRA, accordingly, amended federal law by mandating that the court permit an initial delay only for thirty days, with the option of a ninety-day extension upon a showing of good cause.¹⁵⁰

V. ACCESS TO RECORDS

The ACLU has stated that with the passage of the Patriot Act, “without a warrant and without probable cause, the FBI now has the power to access many private medical records, library records, and student records.”¹⁵¹ There have been repeated claims that the Patriot Act allows the government to do things like go into libraries, make note of what books someone has read, and ensure that he or she is never told about it.¹⁵² In reality, the word “library” cannot be found anywhere in the original Patriot Act. But the above complaints demonstrate the major controversy surrounding the provisions concerning access to records. These authorize the government to obtain an order from a court permitting agents to review and copy records upon

146. 18 U.S.C. § 2705(a).

147. *Id.* § 3103a(b)(3).

148. Patriot Act § 213, 18 U.S.C. § 3103a(b).

149. 18 U.S.C. § 2518(8)(d).

150. PIRA § 213, 18 U.S.C. § 3103a(b)(3).

151. Press Release, ACLU of New Jersey Commends Princeton for Passage of Pro-Civil Liberties Resolution (Oct. 8, 2003), <http://www.aclu.org/safefree/general/17708prs20031008.html>.

152. *E.g.*, Patriot Act Conferences & Meetings, *supra* note 10.

certification that the records are sought for an authorized investigation “to obtain foreign intelligence information” or “to protect against international terrorism or clandestine intelligence activities.”¹⁵³ The provisions contained the same nondisclosure provisions discussed earlier in the context of NSLs,¹⁵⁴ as well as language requiring a judge to issue the order upon receiving the FBI’s request as long as it met the statutory requirements, as opposed to having discretion to accept or reject the application.¹⁵⁵

In fact, the government has always had the ability in ordinary criminal cases to obtain records, from libraries or anywhere else, without probable cause and without telling the target simply by issuing a grand jury subpoena.¹⁵⁶ This subpoena power is routinely authorized by each grand jury as it is impaneled. The subpoenas thereafter are sent out to corporations, banks, individuals, and even libraries any time the agent and the government attorney believe that these entities may have records relevant to an investigation. If a subpoena is challenged, the court will uphold its authority unless “there is no reasonable possibility that the category of materials that the Government seeks will produce information relevant to the general subject of the grand jury’s investigation.”¹⁵⁷ There has never been a requirement of prior court review or approval before these subpoenas are issued and the standard that must be met to justify their use if challenged is, as indicated, very low. There has never been any requirement of probable cause.¹⁵⁸

As national security investigations occasionally may be conducted for intelligence only, as opposed to potential criminal prosecution, there was a need for some mechanism that would allow records to be obtained outside the normal criminal grand jury process. The result was the Patriot Act provision permitting the government to seek court authorization after a certification that the government has a need to review records

153. Patriot Act § 215, 50 U.S.C. § 1861(b)(2).

154. § 215, 50 U.S.C. § 1861(d).

155. § 215, 50 U.S.C. § 1861(c)(1).

156. FED. R. CRIM. P. 17(c).

157. *United States v. R. Enterprises, Inc.*, 498 U.S. 292 (1991).

158. *Id.* at 297 (“[T]he Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists.”).

relevant to a foreign intelligence investigation or to protect against international terrorism and espionage.¹⁵⁹ Because of the mandate that there must be a court order and certification of need, the Patriot Act provision is actually in many respects more restrictive than the standards followed in ordinary criminal cases in which a grand jury subpoena is issued. In fact, not only must a judge review the government's sworn allegation, but the Patriot Act specifically states that the FBI cannot conduct an investigation "of a United States person solely upon the basis of activities protected by the first amendment to the Constitution."¹⁶⁰ This latter requirement would appear to counter public claims that this statute was somehow passed with the intention that the government "could spy on a person because they don't like the books she reads, or because they don't like the web sites she visits."¹⁶¹

Nevertheless, the public clamor surrounding the access-to-records provisions, as well as the previously cited district court opinions on NSLs,¹⁶² resonated with Congress. Unlike some of the Patriot Act objections driven in part by misunderstanding and highly theoretical speculation, the complaints directed toward the access-to-records provisions appeared to have merit. Thus, in PIRA Congress made it clear that, if a judge does not find the statutory requirements had been met, the judge has discretion to reject the government's application for access to records.¹⁶³ Furthermore, the recipient of a request for records was authorized to disclose the request to his lawyer¹⁶⁴ and contest compliance in court.¹⁶⁵ Congress also stated that the recipient could disclose the existence of the application if the court found "no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person."¹⁶⁶ If the recipient was denied the right to

159. Patriot Act § 215, 50 U.S.C. § 1861(b)(2).

160. § 215, 50 U.S.C. § 1861(a)(2)(B).

161. ACLUOhio.org, Free Speech: What's Happening Nationally, <http://www.acluohio.org/issues/FreeSpeech/default.asp> (last visited Apr. 29, 2007).

162. *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004); *Doe v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005).

163. PIRA § 106(c), 50 U.S.C. § 1861(c)(1).

164. § 106(e), 50 U.S.C. § 1861(d)(1)(B).

165. § 106(f)(2), 50 U.S.C. § 1861(f)(1).

166. Patriot Amendments Act § 3, 50 U.S.C. § 1861(f)(2)(C)(i).

disclose, he could petition the court again after twelve months.¹⁶⁷ In addition, despite the fact that grand jury subpoenas do not have to be supported by a government narrative, Congress required that requests for access to records must be supported by facts that lead to a conclusion that the tangible records sought are relevant to a foreign intelligence investigation or that there are specified connections to a foreign power.¹⁶⁸ Finally, for all requests for access to sensitive categories of records, such as library records, tax returns, firearms records, education records, and medical records, there must be high-level government approval and congressional reporting.¹⁶⁹

As a direct result of these amendments to the Patriot Act, the ACLU withdrew a previously filed constitutional challenge to those provisions.¹⁷⁰ The organization stated that it would continue to represent individual recipients who believed they had reasonable grounds to contest the government's order not to disclose a request for records or the receipt of national security letters.¹⁷¹

VI. CONCLUSION

The Patriot Act headlines and sound bites that have permeated the print media and airwaves have created genuine public concern in the United States. An examination of the lengthy articles beneath the headlines in the print media, on the Internet, and in journals unfortunately often reflect the same fear, emotion, and misrepresentations that were originally created by the headlines and sound bites. It is important for lawyers and scholars to stand back and look at the exact provisions of the Patriot Act, consider how they relate to established law, and identify where these provisions are consistent with the Constitution and case law and where they may have reached beyond the boundaries. The district court

167. § 3, 50 U.S.C. § 1861(f)(2)(A)(i).

168. PIRA § 106(b), 50 U.S.C. § 1861(b)(2)(A).

169. § 106(a), 50 U.S.C. § 1861(a)(3).

170. Press Release, Citing Improvements to Law, ACLU Withdraws Section 215 Case But Vows to Fight Individual Orders (Oct. 27, 2006), <http://www.aclu.org/safefree/patriot/27211prs20061027.html> (the ACLU withdrew its suit in *Muslim Cmty. of Ann Arbor v. Ashcroft*, 459 F. Supp. 2d 592 (E.D. Mich. 2006)).

171. *ACLU Ends Business Records Provision Suit, Will Focus Action on Specific Requests, NSLs*, 75 U.S.L.W. 2263 (2006); see also Press Release, Citing Improvements to Law, ACLU Withdraws Section 215 Case But Vows to Fight Individual Orders, *supra* note 170.

opinions that are now emerging, as well as the passage of PIRA, reflect that process. Hopefully the American public will benefit from a more focused and mature, and less emotional and partisan, analysis in the years ahead.