

Notes

THE PATRIOT ACT'S IMPACT ON THE GOVERNMENT'S ABILITY TO CONDUCT ELECTRONIC SURVEILLANCE OF ONGOING DOMESTIC COMMUNICATIONS

NATHAN C. HENDERSON

INTRODUCTION

In the wake of the September 11 terrorist attacks on the World Trade Center and the Pentagon,¹ Congress enacted the USA Patriot Act of 2001.² To achieve the Act's stated objective of making it easier for federal agents to identify and investigate possible terrorist threats,³ Congress modified preexisting surveillance law, which, among other things, established the conditions under which the government could electronically monitor various types of ongoing communications⁴ within the United States in nonemergency situations.⁵

Copyright © 2002 by Nathan C. Henderson.

1. More than three thousand people died during the attacks. *Dead and Missing*, N.Y. TIMES, Jan. 11, 2002, at A11.

2. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter Patriot Act] (codified in scattered titles of U.S.C.).

3. *Id.*, 115 Stat. at 272 (stating that the purpose of the Act is to "deter and punish terrorist attacks . . . [and] enhance law enforcement investigatory tools").

4. The government also has the power to access stored communications, such as stored e-mails or voicemails. 18 U.S.C. § 2703 (2000), *amended by* Patriot Act § 209, 115 Stat. at 283. Since stored communications are accessed after they have already been sent and received, government access does not occur while the communication is actually ongoing. Consequently, any analysis of the government's power to access stored communications is outside the scope of this Note.

5. If, for instance, the government knew that a terrorist attack were imminent, the government might be able to conduct electronic surveillance without a warrant. *See* 50 U.S.C. § 1803(e) (2000) (stating that the government can conduct warrantless electronic surveillance to obtain foreign intelligence information if the Attorney General reasonably determines that an

This body of law is referred to throughout this Note as “electronic surveillance law,” and it is the Patriot Act’s impact on this body of law that is the sole focus of this Note.

This Note argues that, even though some of the Patriot Act modifications to the preexisting electronic surveillance law do not engender significant privacy concerns, the modifications considered in their entirety do pose a threat. The threat, however, is one that is containable, provided that certain precautionary measures are observed until the appropriate statutory reform can occur.

Part I of this Note summarizes the development of electronic surveillance law prior to the enactment of the Patriot Act. Part II details how the Patriot Act modified preexisting law and gauges each modification’s likely impact on privacy. Part III then identifies the Patriot Act modifications that pose the greatest threat to privacy, explains that it is impossible to consider these modifications in isolation, and establishes that, while the Patriot Act does contain some provisions that favor privacy, these provisions are not sufficient to counter the potential threat. Finally, this Note concludes by setting forth what must happen if the threat to privacy is to be minimized.

I. THE DEVELOPMENT OF ELECTRONIC SURVEILLANCE LAW PRIOR TO THE ENACTMENT OF THE PATRIOT ACT

Ever since the invention of the wiretap made electronic surveillance a reality,⁶ the government has justified monitoring certain communications on the grounds that doing so is necessary to properly investigate crime and protect national security.⁷ Congress eventually decided that the conditions under which the government could conduct electronic surveillance depended on the government’s stated objective. If the government sought evidence to be used in a criminal proceeding, one body of law governed.⁸ If the government acted to

emergency exists and that there is insufficient time in which to obtain prior judicial authorization). An analysis of such a scenario, however, is outside the scope of this Note.

6. See Ira Glasser, *The Struggle for a New Paradigm: Protecting Free Speech and Privacy in the Virtual World of Cyberspace*, 23 NOVA L. REV. 625, 638–39 (1999) (“The wire through which [telephone] conversations would pass, was initially thought to be . . . impenetrable. . . . [but] [i]t was clear though that no one had anticipated wiretapping.”).

7. See William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 4 (2000) (observing that “invasions of privacy [may be construed] as necessary evils in enforcing the criminal laws . . . [and in] seek[ing] intelligence information”).

8. See *infra* Part I.A.

protect national security, a related, but different, body of law applied.⁹ Terrorism, though, proved to be an “exception to the general rule” because both bodies of law governed its investigation.¹⁰ Because the Patriot Act was enacted in response to a terrorist attack, this Note summarizes the development of both bodies of law.

A. *Development of the Preexisting Law: Electronic Surveillance Conducted as Part of a Criminal Investigation*

The Fourth Amendment established constitutional protection for “[t]he right of the people to be secure in their persons, houses, papers, and effects,”¹¹ but, prior to 1967, the courts only applied the Amendment’s language literally.¹² For years, the seminal case was *Olmsted v. United States*,¹³ in which the Supreme Court held that privacy was adequately protected by the Fourth Amendment’s emphasis on physical trespass.¹⁴

Then, in 1967, the Supreme Court decided both *Berger v. New York*¹⁵ and *Katz v. United States*.¹⁶ In *Berger*, the Court characterized as offensive any electronic surveillance that was lengthy, continuous, or excessively broad.¹⁷ In *Katz*, the Supreme Court finally overruled

9. See *infra* Part I.B.

10. Banks & Bowman, *supra* note 7, at 9 (noting that terrorism is an exception to the general rule because its “primary, albeit intermediate, objective” is “mayhem and individual harm[],” but its “ultimate objective . . . is the quintessential national security threat—an attack on the United States as a sovereign nation”); see also Ronald J. Sievert, *Meeting the Twenty-First Century Terrorist Threat Within the Scope of Twentieth Century Constitutional Law*, 37 HOUS. L. REV. 1421, 1422–23 (2000) (observing that a “terrorist incident . . . can be a transforming event” that can “have catastrophic effects on American society beyond the [many] deaths it might cause” (quoting *Combating Terrorism: Implementation and Status of the Department of Defense Domestic Preparedness Program: Hearing Before the Subcomm. on Nat’l Sec., Int’l Affairs, and Criminal Justice of the House Comm. on Gov’t Reform and Oversight*, 105th Cong. 50–51 (1998) (statement of Frank Cilluffo, Senior Analyst, Center for Strategic and International Studies))).

11. U.S. CONST. amend. IV.

12. Michelle Skatoff-Gee, *Changing Technologies and the Expectation of Privacy: A Modern Dilemma*, 28 LOY. U. CHI. L.J. 189, 192 (1996) (noting that Fourth Amendment protections only applied when “government agents searched or seized tangible ‘houses, papers, or effects’”).

13. 277 U.S. 438 (1928).

14. *Id.* at 465–66.

15. 388 U.S. 41 (1967).

16. 389 U.S. 347 (1967).

17. See *Berger*, 388 U.S. at 58–60 (holding that the statute was offensive because it did not require any showing that a particular offense had been committed, that the intrusions were essentially a continuous invasion of privacy, and that the surveillance could last for an indefinite period of time). The *Berger* Court also stated that electronic surveillance was inherently intru-

Olmsted and held that wiretapping and other forms of electronic surveillance were subject to the privacy protections of the Fourth Amendment.¹⁸ As Justice Harlan articulated in his concurrence, people are entitled to Fourth Amendment protection if they exhibit “an actual (subjective) expectation of privacy . . . that . . . society [could] recognize as ‘reasonable.’”¹⁹

In response to *Berger* and *Katz* and to law enforcement’s claim that wiretapping was needed to fight crime,²⁰ Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).²¹ In enacting Title III, Congress also sought to protect privacy by establishing uniform conditions under which electronic surveillance could occur.²² Most importantly, Title III established that the government could only intercept the content of wire communications pursuant to a court order based on a finding of probable cause.²³ To obtain authority for a roving wiretap,²⁴ the government also had to show that the surveillance target intended to “thwart interception by changing facilities.”²⁵ In all surveillance cases, Title III mandated that the surveillance target have, prior to the introduction of any damaging evidence in a criminal proceeding, the opportunity to challenge both the existence of probable cause and the conduct of the surveil-

sive because it “[swept] in all conversations within its scope—without regard to the participants or the nature of the conversations.” *Id.* at 65 (noting that a single wiretap resulted in the taping of “conversations involving, at the other end, The Julliard School of Music, Brooklyn Law School, [and a number of other respectable institutions]”).

18. 389 U.S. at 353.

19. *Id.* at 361 (Harlan, J., concurring).

20. James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 71 (1997).

21. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2510–2522 (2000)).

22. Dempsey, *supra* note 20, at 71.

23. 18 U.S.C. § 2518(3) (2000). In addition, the government also had to show both that it had a special need to engage in electronic surveillance, *id.* § 2518(3)(c), and that electronic surveillance could be carried out such that the likelihood of intercepting innocent communications would be minimized, *id.* § 2518(5).

24. Roving wiretaps are “[wire]taps placed on a phone line other than the line subscribed to by the target of a surveillance order” and are considered especially invasive “because they often entail tapping the phone of someone who is not the subject of an investigation and not suspected of any involvement in criminal conduct.” Dempsey, *supra* note 20, at 114.

25. 18 U.S.C. § 2518(11) (1994). This provision was later slightly altered. Now, the government only has to show that the effect of the target’s actions may be to evade interception. *See* 18 U.S.C. § 2518(11)(b)(ii) (2000) (requiring solely that the government show that “the person’s actions could have the effect of thwarting interception”).

lance.²⁶ If such a challenger prevailed, any improperly obtained evidence would be statutorily excluded.²⁷

For the next eighteen years, Title III was the only codified protection for oral and wire communications.²⁸ Technology, however, increasingly began to surge ahead of what statute could protect,²⁹ especially where electronic communications were concerned.³⁰ As a result, communications were subject to “widely disparate legal treatment” depending on the form of the communication.³¹ Recognizing the need for reform, Congress passed the Electronic Communications Privacy Act of 1986 (ECPA)³² in an attempt “to bring [the] new technologies . . . into the statutory framework of the laws governing wiretaps.”³³

ECPA extended the scope of Title III by prohibiting the unauthorized monitoring of electronic communications.³⁴ ECPA also provided some protection for the transactional data that was generated by communications systems by establishing rules for the use of pen

26. *Id.* § 2518(9)–(10)(a).

27. *See id.* § 2515 (stating that no improperly intercepted wire or oral communication can be received in evidence if disclosure would be in violation of Title III); *id.* § 2518(10)(a) (stating that “[a]ny aggrieved person . . . may move to suppress the contents of any wire or oral communication . . . unlawfully intercepted”). In short, this “statutory exclusionary rule provides for the exclusion of wire or oral wiretap evidence if law enforcement violates any ‘central’ provision of Title III, even if the violation is purely statutory and suppression is not required by *Katz* and *Berger*.” Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III’s Statutory Exclusionary Rule and Expressly Reject a “Good Faith” Exception*, 34 HARV. J. ON LEGIS. 393, 408 (1997).

28. Skatoff-Gee, *supra* note 12, at 201.

29. *See id.* (“With the advent of cellular telephones, computer-to-computer transmissions, and electronic mail systems, technology outpaced . . . statutory protections.”).

30. *See Leib, supra* note 27, at 402–03 (“What was perfectly clear . . . was that Title III . . . did not cover electronic communication.”).

31. *Id.* at 403 (quoting Robert W. Kastenmeir et al., *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715, 720). As a result of this omission, business rivals could intercept each other’s “electronic communications . . . without repercussion” and “by the mid 1980s, companies were losing millions of dollars a year to [such] ‘electronic espionage.’” *Id.* at 403–04.

32. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2521, 2701–2709, 3121–3127 (2000)).

33. Leib, *supra* note 27, at 393.

34. 18 U.S.C. § 2511. While it is correct to say that ECPA does not apply to ham or CB radio broadcasts, ECPA may apply to data transfers involving wireless local area networks. *See Dempsey, supra* note 20, at 110 n.233 (“The status of legal protection for wireless data transfers has a confused history, leaving it unclear whether they are currently protected.”).

registers and trap and trace devices.³⁵ ECPA required the government to obtain a court order before installing either device³⁶ unless the government only sought to obtain transactional information relating to the target's electronic communications, in which case a subpoena was sufficient.³⁷ Regardless of what Congress might have intended, however, ECPA as enacted gave less protection to electronic communication than Title III gave to wire and oral communication.³⁸

The passage of ECPA did not halt the advance of technology, and law enforcement soon complained that the new "developments were making . . . interception [of communications] more difficult."³⁹ Congress responded by enacting the Communications Assistance for Law Enforcement Act (CALEA).⁴⁰ The purpose of CALEA was to "preserve the government's ability . . . to intercept communications involving advanced technologies . . . while protecting the privacy of communications and without impeding the introduction of new technologies."⁴¹

35. "[T]he term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached [but does not relate to billing information]." 18 U.S.C. § 3127(3). "[T]he term 'trap and trace device' means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." *Id.* § 3127(4). Throughout this Note, both devices are often collectively referred to as pen/trap devices.

36. *Id.* § 3122(b)(2) (stating that an application for a court order must include the identity of the government official making the request and a "certification . . . that the information likely to be obtained is relevant to an ongoing criminal investigation"). The judge's role in granting a court order for either a pen register or a trap and trace device is purely ministerial. *See id.* § 3123(a) ("[T]he court *shall* enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device . . . if the court finds that the attorney for the Government . . . has [properly] certified [the application]." (emphasis added)). In other words, "the sole function of the judge is to determine whether the signature of a[] [Government attorney] is on the application." Dempsey, *supra* note 20, at 113.

37. 18 U.S.C. § 2703(c)(1)(C).

38. Leib, *supra* note 27, at 406. ECPA allowed federal officials to request interception of electronic communications whenever they thought it would "provide . . . evidence of *any Federal felony*" and provided that "*any government attorney*" could approve such an intercept application. 18 U.S.C. § 2516(3) (emphasis added).

39. Dempsey, *supra* note 20, at 89–90 (attributing the difficulties to (1) the "rapid growth of wireless systems," (2) an increased number of telecommunications service providers, and (3) an expanded menu of call processing options; all of which made it increasingly harder to "isolat[e] the communication stream associated with a particular target").

40. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010 (1994 & Supp. 1999), 18 U.S.C. § 3124 (2000), and in scattered sections of 47 U.S.C.).

41. H.R. REP. NO. 103-827, at 9 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3489.

In CALEA, Congress recognized that the transactional data associated with sending, receiving, and storing e-mail revealed much more about the user than did the digits of a telephone number.⁴² For this reason, Congress ceased to allow such information to be obtained merely by means of a subpoena and began requiring a court order.⁴³ Congress also prohibited the government from using pen/trap authority to obtain any tracking or location information other than that which could be determined from a telephone number.⁴⁴

Between the enactment of CALEA and the passage of the Patriot Act, electronic surveillance law remained relatively unchanged so far as criminal investigations were concerned.

B. Development of the Preexisting Law: Electronic Surveillance Conducted in the Interests of National Security

Even though the Foreign Intelligence Surveillance Act (FISA)⁴⁵ has governed electronic surveillance conducted in the name of national security since 1978, the events that led to the statute's enactment continue to affect debates over the appropriateness of electronic surveillance. Thus, this Note first briefly describes these events before setting forth the relevant provisions of the statute.

1. *Background to FISA.* Through the early 1900s, the executive branch was almost entirely responsible for handling intelligence matters, and Congress deferred to its judgment.⁴⁶ As the world became more complex, however, so too did the threats to national security.⁴⁷ Sadly, the American response was sometimes characterized by a tendency to “tak[e] a few isolated incidents and inflat[e] them into . . . [a]

42. H.R. REP. NO. 103-827, at 31 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3511.

43. *Id.*

44. 47 U.S.C. § 1002(a) (1994).

45. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1811 (1994 & Supp. 1999), 8 U.S.C. § 1101 (2000), 47 U.S.C. §§ 605–606 (1994 & Supp. 1999), and in scattered sections of 18 U.S.C.), amended by Intelligence Authorization Act for Fiscal Year 2000, Pub. L. No. 106-120, 113 Stat. 1606 (1999).

46. See Banks & Bowman, *supra* note 7, at 17–18 (noting that “[t]his approach offended no one, because the nature of intelligence activities rarely touched the private lives of the citizenry”).

47. See *id.* at 19–20 (discussing how the wiretapping of the German and Austro-Hungarian embassies, coupled with interception of the Zimmerman telegram, created fear of domestic subversion in the United States).

vast threat, requiring an immediate, repressive response.”⁴⁸ One such example occurred in 1917, when fear of German subversion caused Congress to enact the Espionage Act of 1917.⁴⁹ The resulting “[v]ague regulations took their aim not at German spies, but at agitators, while legions of informers, private investigators and federal agents combined to root out subversive elements.”⁵⁰ Similarly, “[w]hen a spy scare swept the nation near [the end of World War I],” the Attorney General accepted the volunteer “assistance” of the American Protective League.⁵¹ After each volunteer was given a badge similar to a police shield, the APL conducted a zealous campaign against numerous forms of perceived disloyalty.⁵²

Over time, fear of Germans was gradually displaced by fear of Bolsheviks, and raids on suspected Communists became the new vogue.⁵³ These raids were called “Palmer raids” after the Attorney General who approved them, and they resulted in the arrests of numerous individuals without probable cause.⁵⁴ Some people protested the government’s actions, “but they were few and the perceived red

48. David B. Kopel & Joseph Olson, *Preventing a Reign of Terror: Civil Liberties Implications of Terrorism Legislation*, 21 OKLA. CITY U. L. REV. 247, 252 (1996); see also Thomas I. Emerson, *Symposium: National Security and Civil Liberties: Introduction*, 69 CORNELL L. REV. 685, 685–86 (1984) (“Appeals to patriotism and especially expressions of alarm about the intentions of foreign enemies have always been used as techniques for rallying political support. The resulting tides of public opinion are likely to create a diversion from the real issues that must be resolved.”).

49. See Banks & Bowman, *supra* note 7, at 22 (stating that the Espionage Act, which was enacted on June 15, 1917, “authorized the government to confiscate property, wiretap, search and seize private property, censor writings, open mail and restrict the right of assembly,” despite the fact that “[t]he specter of German subversion far surpassed reality”).

50. *Id.*

51. *Id.* at 23.

52. See *id.* (“Acting without police powers, volunteers conducted arrests . . . tapped telephones and conducted ‘slacker raids’ to root out draft dodgers.”).

53. See Kopel & Olson, *supra* note 48, at 254 (noting that raids of radical groups became more frequent because “[a]s Communists took over Russia following the end of the war, American fears of violent foreign radicals intensified”).

54. Banks & Bowman, *supra* note 7, at 24–25; see also ELLEN SCHRECKER, *THE AGE OF MCCARTHYISM* 11 (1994) (stating that the Palmer Raids “were the culmination of almost a year of near hysteria on the part of politicians, journalists, and businesspeople who claimed that the left wing agitation and labor unrest that had followed World War I threatened to plunge the nation into the revolutionary chaos that they claimed was sweeping Europe”). Even though it might have seemed like a good idea in the aftermath of the Palmer Raids, dismantling the intelligence services completely would have been a “significant error” because intelligence information would soon prove to be critical. See Banks & Bowman, *supra* note 7, at 25 (noting that, at the time, Bolshevism, European Fascism, and “Japanese hegemonic militarism” were movements that already had begun to attract followers).

threat loomed larger than life.”⁵⁵ For this reason, and because *Olmsted* did nothing to restrict the use of wiretaps, the executive branch employed electronic surveillance whenever it thought that doing so was in the national interest.⁵⁶

In 1949, Americans learned that the Soviets possessed nuclear capabilities.⁵⁷ “By the early 1950s . . . Soviet spy rings had been uncovered in the United States, Communists had overrun China and Americans were dying in Korea.”⁵⁸ Public awareness of these events, fanned by the diatribes of Senator Joseph McCarthy, combined to create fear of all things perceived to be Communist.⁵⁹ “Foreign threats were targeted, but so [too] was a domestic fifth column of Americans who were viewed as potential threats to the national security.”⁶⁰ Not surprisingly, by the mid 1950s, “J. Edgar Hoover [had] announced to the FBI that the Bureau was authorized to enter private property for the purpose of installing electronic surveillance devices, without regard for surreptitious entry and without prior authorization from the Attorney General.”⁶¹ Subsequently, President Johnson “‘modified the standard to permit warrantless wiretapping’” when it was necessary to

55. Banks & Bowman, *supra* note 7, at 25.

56. *See id.* at 26–30 (describing the expanding scope and use of electronic surveillance employed between the 1930s and the 1950s). Beginning in 1931, each Attorney General endorsed the use of wiretaps in certain cases. William P. Rogers, *The Case for Wire Tapping*, 63 *YALE L.J.* 792, 794 (1954). Then, in 1940, Attorney General Robert H. Jackson stated that the Department of Justice would no longer use wiretaps or handle cases for other agencies in which wiretaps had been used. *Id.* at 795. This change proved to be only temporary. Shortly thereafter, President Franklin D. Roosevelt wrote to Jackson and “authorized the use of wiretapping in [national] security cases provided in each case [that] the Attorney General gave his specific approval.” *Id.* at 795 n.15. In 1941, President Roosevelt wrote to the House Judiciary Committee to state that it was sometimes necessary to conduct wiretapping to protect the national security of the country. *Id.* at 796.

57. RICHARD POLENBERG, *ONE NATION DIVISIBLE: CLASS, RACE, AND ETHNICITY IN THE UNITED STATES SINCE 1938*, at 97 (1980). The announcement that the Soviets possessed nuclear capability “unleashed a torrent of anxiety and finger-pointing as both policymakers and private citizens struggled to come to terms with these staggering blows to America’s self-confidence and preeminence in the world.” SCHRECKER, *supra* note 54, at 32.

58. Banks & Bowman, *supra* note 7, at 29.

59. *See, e.g.*, POLENBERG, *supra* note 57, at 126 (stating that “McCarthyism sanctioned vicious smear campaigns, created harmful pressures for conformity, and rode roughshod over individual rights, all of which was antithetical to American ideals, if not atypical of American practices”).

60. Banks & Bowman, *supra* note 7, at 30.

61. *Id.* at 28.

protect national security.⁶² On the surface, the Nixon administration claimed to take the same approach. In reality, though, “the President’s men . . . claimed unprecedented authority to conduct electronic surveillance,”⁶³ “us[ing] wiretaps to investigate [both] news leaks” and political opponents.⁶⁴

By the early 1970s, the political climate had begun to shift for several reasons. First, the American public had had time to get used to *Katz*, and even though the *Katz* Court did not consider the national security aspect of electronic surveillance,⁶⁵ the opinion arguably helped cement into the public consciousness the idea that privacy was an essential element of democracy. Second, in *United States v. United States District Court* (*Keith*⁶⁷), the Supreme Court finally answered the question it had left unanswered in *Katz* and held that the Fourth Amendment prohibited warrantless surveillance that targeted domestic threats to national security.⁶⁸ Third, Americans gradually began to realize that their government had monitored many of them without their knowledge,⁶⁹ and this realization made many of them angry.⁷⁰

62. Gerald F. Reimers II, *Foreign Intelligence Surveillance Act*, J. NAT'L SECURITY L. 55, 63 (2000) (quoting Steven Saltzburg, *National Security and the Fourth and Fifth Amendments*, in NATIONAL SECURITY LAW 1001, 1019 (John Norton Moore et al. eds., 1990)).

63. CARL BERNSTEIN & BOB WOODWARD, ALL THE PRESIDENT'S MEN 258 (1974).

64. See *id.* at 313 (noting that, between 1969 and 1971, the Nixon administration tapped the telephones of both government officials and reporters).

65. See *Katz v. United States*, 389 U.S. 347, 358 n.23 (1967) (“Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.”).

66. 407 U.S. 297 (1972).

67. This case came to be known as *Keith* because Judge Damon J. Keith was the federal district judge that heard the case. Robert A. Dawson, *Shifting the Balance: The D.C. Circuit and the Foreign Intelligence Surveillance Act of 1978*, 61 GEO. WASH. L. REV. 1380, 1384 n.20 (1993).

68. 407 U.S. at 320. Ironically, *Keith* was decided two days after the Watergate arrests. BERNSTEIN & WOODWARD, *supra* note 63, at 258.

69. For example, “the NSA was known to have conducted an extensive monitoring program under the code name Shamrock through which the agency received copies of most international telegrams leaving the United States between 1945 and 1975.” Eric M. Freedman, *Freedom of Information and the First Amendment in a Bureaucratic Age*, 49 BROOK. L. REV. 835, 841 n.16 (1983). Further, since “a Senate Committee conducted a full investigation of the interception program and prepared a detailed report that was later read into the record,” nothing remained secret about the operation. *Id.*; see also Banks & Bowman, *supra* note 7, at 31 (noting that surveillance operations like Operation Shamrock “came to an end only when congressional interest in intelligence activities began to focus on privacy issues” and were only disclosed when “public hearings [became] a certainty”). Also, Title III required the government to keep track of its wiretapping activities and disseminate the resulting information in report format. 18 U.S.C. § 2519 (2000). The data that the government collected certainly seems like it would have focused the public’s attention. See Glasser, *supra* note 6, at 642 (“In the first four years after the

Fourth, oversight committees began to criticize the intelligence community for the methods it had used.⁷¹ These committees did not have an immediate impact, but they did create a “first-time focus on the President’s authority for national security surveillance.”⁷² Most significantly though, the publication of the Pentagon Papers and the coverage of the Watergate scandal caused many people to question the authority claimed by the executive branch.⁷³

2. *FISA*. In *Keith*, Justice Powell had invited Congress to regulate domestic security surveillance.⁷⁴ In 1978, Congress accepted Justice Powell’s invitation and enacted the Foreign Intelligence Surveil-

1968 bill was passed, 1.1 million conversations were overheard, 93,080 people were spied upon, 6131 people were arrested and a total of 1154 people were reported convicted—barely more than one percent.”).

70. People had good reason to be angry. The newspapers had published stories of how dissident groups in the United States had been the targets of electronic surveillance, break-ins, and mail openings. Reimers, *supra* note 62, at 64. Worse yet, “[a]dditional disclosures began to surface in [the mid 1970s] with regard to the CIA’s domestic operations and the efforts of the FBI to undermine the activities of Rev. Martin Luther King and other civil rights leaders during the 1960s.” *Id.* (quoting Daniel B. Silver, *Intelligence and Counterintelligence*, in NATIONAL SECURITY LAW 913, 920 (John Norton Moore et al. eds., 1990)).

71. The Rockefeller Commission, which had been created by President Ford, found that if the CIA’s purpose was “the prosecution of crimes or protection against civil disorders of domestic insurrection, then the activity [usually should have been] prohibited.” Banks & Bowman, *supra* note 7, at 33 (quoting COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES, REPORT TO THE PRESIDENT 62 (1975)). Similarly, the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, which was known as the Church Committee, found “multiple shortcomings in intelligence operations, adverse effects of secrecy, failure by Congress to oversee intelligence activities, and in some cases, seemingly unlawful actions.” *Id.* (footnotes omitted). The Church Committee ultimately “determined that secret government activities, while necessary to the effectiveness of government, were, nevertheless, a threat to democratic society” and that “[t]he remedy . . . was to have Congress prescribe rules for intelligence activities.” *Id.*

72. *Id.*

73. *See id.* (stating that “it was only natural that with new awarenesses, the public began to challenge intelligence activities as never before”); DAVID W. LEVY, THE DEBATE OVER VIETNAM 162 (1991):

Perhaps as damning in the eyes of the public as the content of the [Pentagon] papers was the unseemly way that the Nixon administration scrambled to prevent their publication. By the time the Supreme Court decided that they could be printed, many Americans . . . were perfectly certain that they must contain some pretty damaging information.

74. *See United States v. U.S. Dist. Court*, 407 U.S. 297, 322 (1972) (“Given [the] potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III.”).

lance Act (FISA).⁷⁵ The legislative history established that Congress was in large part responding to the “revelations that warrantless electronic surveillance in the name of national security [had] been seriously abused.”⁷⁶ At the same time, Congress also realized that “[s]afeguarding national security . . . [was] a vitally important Government purpose,” and that it was legislating in a “dangerous world” containing any number of “hostile intelligence activities.”⁷⁷ For these reasons, Congress chose to limit, as opposed to completely eliminate, the ability of the executive branch to conduct electronic surveillance for national security purposes.⁷⁸

Congress accomplished this objective by requiring federal officers to submit to judicial supervision of their domestic security surveillance activities. Specifically, FISA established a special court (the FISA Court) to review applications requesting electronic surveillance.⁷⁹ In all cases, applications had to be submitted by a federal officer, approved by the Attorney General,⁸⁰ and descriptive of the intended target.⁸¹ Applications also had to establish probable cause that the target was either a foreign power⁸² or the agent of a foreign

75. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1811 (1994 & Supp. 1999), 8 U.S.C. § 1101 (2000), 47 U.S.C. §§ 605–606 (1994 & Supp. 1999), and in scattered sections of 18 U.S.C.), *amended by* Intelligence Authorization Act for Fiscal Year 2000, Pub. L. No. 106-120, 113 Stat. 1606 (1999).

76. S. REP. NO. 95-604, pt. 1, at 7 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908 (“[While] [t]he Federal Government has never enacted legislation to regulate the use of electronic surveillance within the United States for foreign intelligence purposes . . . the Executive Branch and the Congress [recognize] that the statutory rule of law must prevail.”).

77. *Id.* at 9, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3910.

78. *See id.*:

[T]he Executive Branch of Government should have, under proper circumstances and with appropriate safeguards, authority to acquire important foreign intelligence information by means of electronic surveillance. The committee also believes that the past record and the state of the law in the area make it desirable that the Executive Branch not be the sole or final arbiter of when such proper circumstances exist. [FISA] is designed to permit the Government to gather necessary foreign intelligence information by means of electronic surveillance but under limitations and according to procedural guidelines which will better safeguard the rights of individuals.

79. 50 U.S.C. § 1803(a) (1994). This special court consists of seven federal district judges, each from a different district. *Id.* Decisions of the court can be appealed to a designated three-judge panel and then to the Supreme Court. *Id.* § 1803(b). Provided that an application complies with FISA, the reviewing judge shall issue the order. *Id.* § 1805(a). “Under Title III, by contrast, a judge retains discretion to reject an application . . . even if he determines that probable cause exists.” Dawson, *supra* note 67, at 1393 (referencing 18 U.S.C. § 2518(3) (1994)).

80. 50 U.S.C. § 1804(a).

81. *Id.* § 1804(a)(3).

82. *Id.* § 1804(a)(4)(A). A “foreign power” is defined as a “foreign government . . . whether or not recognized by the United States,” an entity controlled by a foreign government,

power,⁸³ and that “each of [the locations at which surveillance was to be conducted was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power.”⁸⁴

If the target was a foreign power,⁸⁵ the application had to contain a certification that (1) the information sought was foreign intelligence information,⁸⁶ (2) the purpose of the surveillance was to obtain such information, and (3) the information could not be obtained by normal investigative techniques.⁸⁷ In addition, the application had to both describe the proposed minimization procedures⁸⁸ and state the “period

or “a group engaged in international terrorism or activities in preparation therefore.” *Id.* § 1801(a)(1)–(6). International terrorism is defined as “activities that involve . . . acts dangerous to human life that are a violation of the criminal laws of the United States [and that] appear to be intended to intimidate or coerce a civilian population . . . [or] government, [the consequences of which] transcend national boundaries.” *Id.* § 1801(c).

83. *Id.* § 1804(a)(4)(A). An “agent of a foreign power” is defined as *any person other than a United States person* who acts in the United States as an officer, employee, or member of a foreign power or who “engages in clandestine intelligence activities in the United States contrary to the interests of the United States.” *Id.* § 1801(b) (emphasis added).

Section 1801(i) defines a U.S. person as being one of the following: (1) a U.S. citizen, (2) an alien lawfully residing permanently in the United States, (3) an unincorporated association that is not a foreign power and that has a substantial number of members that satisfy either (1) or (2), or (4) a corporation that is not a foreign power and is incorporated in the United States. Throughout this Note, the phrases “U.S. person” and “non U.S. person” are used to denote whether entities meet the preceding definition.

An “agent of a foreign power” is also defined as “*any person* who knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power [and whose] activities involve or may involve a violation of the criminal statutes of the United States” or any person who “*knowingly engages in sabotage or international terrorism*” or who “*knowingly assumes a false or fraudulent identity for or on behalf of a foreign power*” or who “*knowingly conspires* with any person to engage in [any of the activities described above].” *Id.* § 1801(b) (Supp. V 1999) (emphasis added). That said, “no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.” *Id.* § 1805(a)(3)(A) (1994). Note that, “unlike in Title III, the Executive does not have to demonstrate that the target’s activity will, or may, result in a specific criminal violation. FISA allows a surveillance application to be approved upon [the lower standard] that a person’s activities ‘may involve’ criminal ‘activity.’” Dawson, *supra* note 67, at 1393.

84. 50 U.S.C. § 1804(a)(4)(B).

85. *Id.* § 1804(b) (stating that applications targeting foreign powers need not “contain the information required by paragraphs (6), (7)(E), (8) and (11) of subsection (a) of this section”).

86. The definition of “foreign intelligence information” depends on whether the target is a U.S. person. *Id.* § 1801(e)(1). If a surveillance target is a U.S. person, “foreign intelligence information” is information that is “necessary” for the government to obtain to protect national security. *Id.* § 1801(e). If a target is not a U.S. person, information is “foreign intelligence information” so long as it just “relates” to national security. *Id.*

87. *Id.* § 1804(a)(7)(A)–(D).

88. *Id.* § 1804(a)(5).

of time for which the electronic surveillance [was] required.”⁸⁹ If the target was an agent of a foreign power, then the application had to be even more detailed.⁹⁰

Information obtained under FISA’s provisions could be disclosed for law enforcement purposes only if either the information was to be used in a criminal proceeding and the Attorney General had given advance authorization,⁹¹ or if the government could establish that intelligence gathering had been the “primary purpose” of the surveillance.⁹² Prior to the introduction of any such information as evidence, the government had to give reasonable notice to the defendant that he or she was the target of FISA surveillance.⁹³ The defendant could then move to suppress the evidence on the ground that the “surveillance was not lawfully authorized or conducted.”⁹⁴ If the Attorney General filed an affidavit stating that disclosure would “harm the national security of the United States,” the district court had to review the application, order, and related materials “in camera and ex parte” to determine whether the surveillance was lawful.⁹⁵ The court was only required to disclose to the defendant such portions of the surveillance materials necessary “to make an accurate determination of the legality of surveillance.”⁹⁶

89. *Id.* § 1804(a)(10). In the case of a foreign power, an application also must summarize the likely impact of the surveillance on U.S. persons so that the court can properly “assess the proposed minimization procedures.” *Id.* § 1804(b).

90. If the target was an agent of a foreign power, the application had to satisfy several additional requirements. First, the application had to describe the nature of the information sought and the type of communications that would be subjected to surveillance. *Id.* § 1804(a)(6). Second, it had to establish the government’s basis for concluding that the information sought was “the type of foreign intelligence information designated” and that it could not be obtained by normal investigative techniques. *Id.* § 1804(a)(7)(E). Third, the application had to describe how the surveillance would be conducted. *Id.* § 1804(a)(8). Finally, if more than one surveillance device was to be used, the application had to specify the minimization procedures that would apply to each device. *Id.* § 1804(a)(11).

91. *Id.* § 1806(b).

92. *E.g.*, *United States v. Pelton*, 835 F.2d 1067, 1076 (4th Cir. 1987) (holding that the evidence gathered was admissible because the primary purpose for collecting it was to gather foreign intelligence information); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (same); Reimers, *supra* note 62, at 91–94 (discussing various tests for determining the “primary purpose” of government surveillance); *see also* *United States v. Cavanagh*, 807 F.2d 787, 791 (9th Cir. 1987) (finding no merit to petitioner’s contention that “he [was] entitled to suppression simply because evidence of his criminal conduct was discovered incidentally as the result of an intelligence surveillance”).

93. 50 U.S.C. § 1806(c).

94. *Id.* § 1806(g).

95. *Id.* § 1806(f).

96. *Id.*

In the more than twenty years that have passed since FISA was enacted, only two applications have been rejected.⁹⁷ Moreover, while the Supreme Court has never considered whether the balance struck by FISA is constitutional, the lower courts have repeatedly “upheld FISA’s constitutionality from just about every angle of attack.”⁹⁸

In 1998, Congress amended FISA to permit the use of pen/trap devices in intelligence-related surveillance.⁹⁹ Otherwise though, the electronic surveillance provisions in FISA remained essentially the same until the Patriot Act was enacted.

97. STEVEN DYCUS ET AL., NATIONAL SECURITY LAW 696 (3d ed. 2002).

98. Reimers, *supra* note 62, at 77–78 (stating that FISA fulfills both the “reasonable” and “warrant” requirements of the Fourth Amendment); *see also* Dawson, *supra* note 67, at 1395–96 (“The view expressed by the Second Circuit in *United States v. Duggan* is representative: ‘We regard the procedures fashioned in FISA as a constitutionally adequate balancing of the individual’s Fourth Amendment rights against the nation’s need to obtain foreign intelligence information.’” (quoting *Duggan*, 743 F.2d 59, 73 (2d Cir. 1984))).

From 1978 “[t]hrough 1987, the FISA Court . . . reviewed over 4000 government applications for approval of electronic surveillance. Only one was rejected. In addition, ‘no court that [was] required to determine the legality of a FISA surveillance under 1806(f) . . . found disclosure or an adversary hearing necessary.’” Dawson, *supra* note 67, at 1396–97 (“It is possible to draw divergent conclusions from this data. One could infer that the extensive FISA safeguards have forced the Executive to self-censor its requests. One could also argue, however, that the courts act merely as a ‘rubber stamp’ whenever the Executive invokes national security.”).

99. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2404 (1998) (codified at 50 U.S.C. § 1842 (1994 & Supp. 1999)). The relevant provision provided that the government had to “demonstrate” that the device to be monitored had been, or was about to be, used in activities that “involve[d] or [might] involve a violation of the criminal laws.” *Id.*; *see also* Banks & Bowman, *supra* note 7, at 80 (observing that the FISA standard required “more of the [government] than the traditional criminal law enforcement rule for using the same surveillance techniques”).

II. THE PATRIOT ACT MODIFIED PREEXISTING ELECTRONIC SURVEILLANCE LAW IN FIVE SIGNIFICANT WAYS¹⁰⁰

A. *When Trying to Obtain an Intercept Order, It May Now Be Easier to Use FISA to Circumvent Title III.*

In the past, a common question that frequently arose where FISA was concerned was “whether [the statute], which naturally would be utilized to obtain ‘foreign intelligence’ information regarding terrorists and spies, [could] be used to identify and criminally convict those same terrorists and spies.”¹⁰¹ The statute itself established one method by which this could be done: information obtained under FISA’s provisions could be disclosed for law enforcement purposes if the information was to be used in a criminal proceeding, and if the Attorney General had given advance authorization.¹⁰² The question still remained though because it was hard, at the beginning of, say, a domestic terrorist investigation, for the government to know how close it actually was to being able to go to trial.¹⁰³ Prosecution of the surveillance target might seem only to be a distant dream, and the government might not have enough evidence to obtain a Title III intercept order.¹⁰⁴ The courts responded to this situation by allowing evidence to be used in criminal trials that was discovered “inciden-

100. Some of the Patriot Act modifications raise only minor concerns because the magnitude of the modification is minimal. For example, the Patriot Act adds terrorist acts to the list of crimes for which a Title III wiretap is obtainable. Patriot Act, Pub. L. No. 107-56, § 201, 115 Stat. 272, 278 (2001). Since the list of predicate crimes already included offenses such as murder, kidnapping, and “crime dangerous to life, limb or property,” 18 U.S.C. § 2516(2) (1994), this modification is likely to have little effect. Similarly, neither changing the maximum period for which FISA surveillance (of a non-U.S. person) can be approved by thirty days, Patriot Act § 207, 115 Stat. at 282, nor increasing the number of FISA judges to eleven, *id.* § 208, 115 Stat. at 282, is that consequential either.

101. Sievert, *supra* note 10, at 1437–38.

102. 50 U.S.C. § 1806(b) (1994).

103. See *United States v. U.S. Dist. Court*, 407 U.S. 297, 322 (1972):

The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government’s preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

104. Sievert, *supra* note 10, at 1438 (noting that it may be hard to show that there is “probable cause to believe that a particular individual will be using a specific communication device to further known criminal activity”).

tally” to FISA surveillance.¹⁰⁵ That is, information obtained pursuant to FISA could be used in criminal proceedings provided that intelligence gathering was the “primary purpose” of the surveillance.¹⁰⁶

The Patriot Act altered the “primary purpose” requirement, and FISA surveillance requests no longer have to establish that intelligence gathering is “the” purpose of the surveillance.¹⁰⁷ All that is required now is that intelligence gathering be a “significant” purpose.¹⁰⁸

This modification has been criticized because it makes it easier for the government to skirt what are supposed to be limitations on permissible domestic surveillance.¹⁰⁹ Some commentators have gone so far as to characterize the blurring between Title III and FISA as “tear[ing] down legal fire walls erected 25 years ago during the Watergate era, when the nation was stunned by disclosures about presidential abuses of domestic intelligence gathering.”¹¹⁰ In short, the concern is that the government might use its newly expanded authority with insufficient discretion.

Some of this criticism may be excessive, especially given that a suspect in the September 11 attacks may have escaped prior detection due to a primary purpose concern.¹¹¹ Moreover, the United States had

105. *United States v. Cavanagh*, 807 F.2d 787, 791 (9th Cir. 1987).

106. *See, e.g., United States v. Pelton*, 835 F.2d 1067, 1075–76 (4th Cir. 1987) (allowing evidence collected by FISA authorized surveillance to be used in a criminal proceeding because the primary purpose of the surveillance was to obtain foreign intelligence information); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (finding that information obtained under FISA is admissible even where “the government [could actually] anticipate that the fruits of [FISA] surveillance [might] later be used . . . as evidence in a criminal trial”).

107. Patriot Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (2001).

108. *Id.*

109. *See* DYCUS ET AL., *supra* note 97, at 690 (questioning whether the FBI is “now permitted to conduct a secret search or wiretap for the primary purpose of investigating a crime even though there is no probable cause to suspect the commission of a crime”); American Civil Liberties Union, *USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances*, at <http://www.aclu.org/congress/1110101a.html> (Nov. 1, 2001) (on file with the *Duke Law Journal*) (“This provision authorizes unconstitutional physical searches and wiretaps . . . without probable cause of crime.”).

110. 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; *see also* Jeffrey Toobin, *Crackdown: Should We Be Worried About the New Antiterrorism Legislation?*, NEW YORKER, Nov. 5, 2001, at 57:

The [Patriot Act] . . . breaks down Cold War-era barriers between foreign intelligence and domestic law enforcement to an unprecedented degree. The Justice Department and other agencies will be permitted to move faster, probe deeper, and strike harder at those suspected of terrorist activities. The corresponding worry is whether these changes will . . . raise the level of fear that citizens feel toward their own government.

111. *See* David Johnston & Philip Shenron, *FBI Curbed Scrutiny of Man Now a Suspect in*

just experienced an attack unprecedented in its magnitude, and national security was threatened. In enacting section 218 of the Patriot Act, Congress was in effect saying that wiretaps should be approved whenever law enforcement, subject to judicial supervision, can establish that a threat to national security exists. Perhaps there was a better way whereby Congress could have maintained the old standards and still ensured that federal agencies would be able to investigate terrorism as needed, but there is no indication that any such solution was then apparent.

In addition, electronic surveillance law today is far removed in many respects from what it was during the Watergate era. Before Watergate, the executive branch essentially just monitored people whenever it thought that doing so was in the national interest.¹¹² Since FISA was enacted, however, government agencies investigating national security threats have had to submit to judicial supervision of their domestic security surveillance activities.¹¹³ The Patriot Act did not change the fact that, if the executive branch cannot satisfy the threshold requirements, the designated judge will refuse to authorize surveillance.¹¹⁴ Granted, what can happen to the information once it has been obtained has changed, but this is not the same thing as the complete absence of judicial involvement.

Still, the statute can be improved. Executive power needs to be checked by that of another branch. Ideally, Congress would make this expressly clear in the statute.¹¹⁵ Until then, however, judges must hold that their giving substantive meaning to “significant” is necessarily implied when they decide whether to admit information obtained

the Attacks, N.Y. TIMES, Oct. 5, 2001, at A1 (stating that the FBI refrained from criminally investigating Zacarias Moussauoui after learning that Moussauoui had stated that he wanted to learn to fly jets but had no interest in landing them, on the ground that starting a criminal investigation might make it difficult to later obtain approval for covert FISA surveillance).

112. See *supra* Part I.B.1.

113. See *supra* notes 79–90 and accompanying text.

114. See *supra* Part I.B.2. More specifically, none of the FISA information that could conceivably be used to convict an individual can be obtained from the individual without initial judicial approval of the government’s claim that there is a threat to national security. See *supra* note 79 and accompanying text.

115. Congress has shown some indication of being dissatisfied, at least in part, with what it created. The House Judiciary Committee has ordered the Department of Justice to respond to a set of written questions by September of 2002. Steve Schultze, *Sensenbrenner Wants Answers on Act; He Threatens to Subpoena Ashcroft to Get Details on Patriot Act*, MILWAUKEE J. SENTINEL, Aug. 20, 2002, at 7A. The written questions ask the Department of Justice both to clarify the extent of the electronic surveillance it has conducted pursuant to the Patriot Act and explain what protections are in place to protect constitutional freedoms. *Id.*

from FISA in a criminal proceeding.¹¹⁶ Independent judicial authority would then subtly check executive power, which is all that FISA was ever intended to accomplish. The executive branch would still be able to protect national security, but people in the United States could be more certain that what is being investigated is actually a national security threat.

B. FISA Courts Can Now Authorize Roving Surveillance.

Before the Patriot Act was enacted, roving wiretaps were only available in the law enforcement context, and, to obtain one, the government had to show that the target was actually using the line to be tapped.¹¹⁷ The Patriot Act changed this. The government now has the power to engage in roving surveillance¹¹⁸ in the intelligence context as well (i.e., pursuant to FISA), but it no longer has the corresponding obligation to demonstrate that the target actually uses the device to be tapped.¹¹⁹

Roving surveillance is highly invasive,¹²⁰ and, not surprisingly, this modification has been resoundingly criticized by privacy advocates. More specifically, this modification has been characterized as a “broad expansion of power” that does not build in “a necessary privacy protection,” with the risk that innocent users could have their privacy invaded.¹²¹ For example, if a terrorist “us[ed] the Internet

116. See Electronic Frontier Foundation, *EFF Analysis of the Provisions of the USA Patriot Act That Relate to Online Activities*, at http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (Oct. 31, 2001) (on file with the *Duke Law Journal*) (stating that if the antiterrorism laws are either “misused to spy on innocent people” or “misused to harm the rights of ordinary Americans involved in low level crimes unrelated to terrorism,” the courts should both punish those responsible and exclude any evidence collected as a result).

117. 18 U.S.C. § 2518(12) (2000).

118. Roving surveillance occurs when the government continuously monitors multiple communications devices pursuant to the same intercept order. *United States v. Hermanek*, 289 F.3d 1076, 1087 (9th Cir. 2002); Dempsey, *supra* note 20, at 114.

119. See Patriot Act, Pub. L. No. 107-56, § 206, 115 Stat. 272, 282 (2001) (stating that the government must show that the target is likely to “thwart” surveillance that focuses on monitoring a single device); Electronic Frontier Foundation, *supra* note 116 (noting that federal agents “can now go from phone to phone, computer to computer without demonstrating that each is even being used by a suspect or target of an order”).

120. See Michael Goldsmith, *Eavesdropping Reform: The Legality of Roving Surveillance*, 1987 U. ILL. L. REV. 401, 416 (noting that “persons speaking with the target . . . are exposed to initial intrusion without a showing of probable cause”).

121. American Civil Liberties Union, *How the Anti-Terrorism Bill Limits Judicial Oversight of Telephone and Internet Surveillance*, at <http://www.aclu.org/congress/1102301g.html> (Oct. 23, 2001) (on file with the *Duke Law Journal*).

connection at a public library and law enforcement was using a FISA wiretap order to monitor his or her Internet communications, [law enforcement] might continue to monitor all Internet communications at that site [even] after the terrorist [had] left and was no longer using the computer.”¹²²

Granted, this modification worked a significant change in the preexisting law, but Fourth Amendment limits on government authority are most likely not exceeded, because the threat to privacy described above appears to be outweighed by the government’s duty to protect national security.¹²³ Several observations are particularly relevant. First, roving surveillance has already been upheld as constitutional in the law enforcement context.¹²⁴ Second, terrorists are likely to become, if they are not already, sophisticated enough to avoid non-roving surveillance.¹²⁵ Third, the government may have the capacity to obtain useful information as a result of being able to monitor individuals suspected of posing a threat to the United States.¹²⁶ Fourth, the threat to privacy is limited in time, since the section of the Patriot Act that authorizes roving FISA surveillance will sunset in 2005.¹²⁷

Although it seems that the benefits to allowing roving surveillance in the FISA context outweigh the burdens, the statute could be improved. More specifically, the privacy concern could be minimized if additional judicial involvement were mandated. At present, the

122. *Id.*

123. *See* United States v. U.S. Dist. Court, 407 U.S. 297, 315 (1972) (establishing the relevant test).

124. While the Supreme Court has not decided whether roving wiretaps violate the Fourth Amendment, several lower courts have upheld their use. *United States v. Hermanek*, 289 F.3d 1076, 1087 (9th Cir. 2002); *United States v. Gaytan*, 74 F.3d 545, 553 (5th Cir. 1996); *United States v. Bianco*, 998 F.2d 1112, 1121 (2d Cir. 1993).

125. Part of the reason law enforcement supported making roving surveillance possible under Title III was that criminals had become increasingly sophisticated about detecting possible surveillance. *Hermanek*, 289 F.3d at 1087 (noting that roving surveillance enabled law enforcement to cope with cellular technology); *see also* Goldsmith, *supra* note 120, at 410 (“The success of electronic surveillance prompted experienced targets to shift telephones continuously, carefully guard conspiratorial meeting sites, and frequently change the locations of meetings.”). If this was true of criminals in general, it almost certainly seems like it would be true of people who threaten national security as well. As Senator Orrin Hatch noted, “Terrorists . . . don’t pay any attention to . . . antiquated laws. They just buy 10 cell phones, talk for a while, [and then discard them as needed].” Adam Clymer, *A Nation Challenged: The Legislation; Antiterrorism Bill Passes; U.S. Gets Expanded Powers*, N.Y. TIMES, Oct. 25, 2001, at A1.

126. *See* Goldsmith, *supra* note 120, at 410 (noting that past surveillance operations indicate that some targets engage in “pertinent discussions on a continuous basis—regardless of location”).

127. Patriot Act, Pub. L. No. 107-56, § 224, 115 Stat. 272, 295 (2001).

judge is not required to monitor roving FISA surveillance. If federal agents were required to report back to the authorizing judge periodically, there would be less chance that the executive branch could abuse the authority with which it has been entrusted, as there would be a greater degree of independent review present. Since the procedural burden on the government would not be excessive, it makes sense to improve the statute in this way.

C. The Standard Under Which FISA Pen/Trap Orders Can Be Obtained Is Now Lower.

To obtain a FISA order authorizing the use of a pen/trap device, the government now only has to certify that the information sought is relevant to an ongoing intelligence or terrorism investigation.¹²⁸ In the past, the government also had to demonstrate that the device to be monitored was likely to be used by someone involved in terrorism or intelligence activities that could violate U.S. criminal laws.¹²⁹ Ironically, the old FISA standard required more of the government than did the corresponding Title III provision.¹³⁰ The Patriot Act thus had the effect of setting virtually the same standard for FISA that existed for Title III.¹³¹

By making it easier for the government to obtain a FISA pen/trap order, Congress increased the likelihood that American citizens will be subject to increased FISA pen/trap surveillance.¹³² While this modification represents a marked change from preexisting law, it does not seem that the consequences will be that severe. Obtaining a pen/trap order under Title III has always been so easy to do,¹³³ that it

128. *Id.* § 214, 115 Stat. at 286.

129. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2404 (1998) (codified at 50 U.S.C. § 1842 (1994 & Supp. 1999)).

130. Banks & Bowman, *supra* note 7, at 80.

131. *See* 18 U.S.C. § 3122(b)(2) (2000) (requiring that an application for a Title III court order approving pen/trap surveillance certify “that the information likely to be obtained is relevant to an ongoing criminal investigation”).

132. Electronic Frontier Foundation, *supra* note 116.

133. 18 U.S.C. § 3123(a) provides that “the court *shall* enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device . . . if the court finds that the attorney for the Government . . . has [properly] certified [the application].” (Emphasis added.) Consequently, the court’s role has been purely ministerial. *United States v. Fregoso*, 60 F.3d 1314, 1320–21 (8th Cir. 1995); *see also* *United States v. Hallmark*, 911 F.2d 399, 402 (10th Cir. 1990) (stating that the judicial role should be limited); *In re Application of the United States for an Order Authorizing the Installation & Use of a Pen Register*, 846 F. Supp. 1555, 1558–59 (M.D. Fla. 1994) (holding that the court’s role with respect to trap and trace devices is limited to confirming: (1) the identity of the applicant and investigating agency, and (2) that the applicant

seems unlikely that the government was ever unable to obtain a pen/trap order when it sought to do so. Thus, any additional intrusion on privacy that occurs as a result of this modification will probably not be nearly invasive enough to be considered much of a threat. Even if it were, however, the additional intrusion would hopefully be offset by an increased ability to protect national security.

In addition, making it easier to conduct pen/trap surveillance under FISA may result in the government having to seek fewer intercept orders. This could happen if the government had cause to suspect a person of terrorist-related activity but was not yet ready to obtain a FISA intercept order. In such a case, the government could conduct pen/trap surveillance, and if the surveillance yielded nothing suspicious and if no further information could be developed, the government might conclude that its suspicions had been misplaced, and end the investigation. If pen/trap surveillance were not a ready option, the tendency might instead be to simply obtain a FISA intercept order. Because intercepting the content of communications is much more invasive than monitoring transactional information, this modification may have the effect of permitting an increased number of minor intrusions, but sometimes rendering unnecessary intrusions that would be much more invasive.

D. Pen/Trap Orders Now Apply to Both Wire and Electronic Communications.

Prior to the enactment of the Patriot Act, there was an ongoing debate as to whether the pen/trap statutes applied only to wire communications or to both wire and electronic (e.g., Internet) communications.¹³⁴ At issue was whether transactional information inherent to

has certified that the information sought is relevant to an ongoing investigation). Moreover, the available data indicates that the government has an almost perfect record for obtaining FISA intercept orders when it applies for them. *See supra* note 97 and accompanying text.

134. When Congress enacted the relevant provision of the original pen/trap statutes codified at 18 U.S.C. § 2703(c), it did not anticipate the “dramatic expansion in electronic communications that would [follow].” COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, U.S. DEP’T OF JUSTICE, FIELD GUIDANCE ON NEW AUTHORITIES THAT RELATE TO COMPUTER CRIME AND ELECTRONIC EVIDENCE ENACTED IN THE USA PATRIOT ACT OF 2001, <http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm> (last updated Nov. 5, 2001) (on file with the *Duke Law Journal*) [hereinafter FIELD GUIDANCE]. “Thus, the statute contained certain language that appeared to apply to telephone communications and that did not unambiguously encompass communications over computer networks. . . . [C]ertain . . . litigants . . . challenged the application of [the ECPA] to . . . electronic communications based on the statute’s telephone-specific language.” *Id.*

communicating electronically was more revealing than the digits dialed on a telephone.¹³⁵ The Patriot Act resolved this ongoing debate by clarifying that the pen/trap statutes apply to both types of communications, so long as content information is excluded.¹³⁶ Because a number of courts had in effect already reached this same conclusion,¹³⁷ this modification is unlikely to entail any significant substantive consequences other than making explicit that which was previously assumed.

Moreover, it is possible to view this modification as not unduly intruding on privacy, because using pen/trap orders to obtain noncontent information relating to electronic communications is often less intrusive than using pen/trap orders to monitor telephone numbers dialed.¹³⁸ Ever since ECPA became law in 1986, the use of pen/trap

135. “‘The Internet is what is known as a packet-switched network,’” which means that “‘there is no single, unbroken connection between sender and receiver,’” and thus, “‘when information is sent, it is broken into small packets, sent over many different routes at the same time, and then reassembled at the receiving end.’” Paul Taylor, *Issues Raised by the Application of Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks*, 6 VA. J.L. & TECH. 4, ¶ 13 (2001), at <http://www.vjolt.net/vol6/issue1/v6i1a04-Taylor.html> (emphasis omitted) (quoting PRESTON GRALLA, HOW THE INTERNET WORKS 13 (1999)). Content information is defined as “any information concerning the substance, purport, or meaning of [a] communication,” 18 U.S.C. § 2510, and the “packet-switched” nature of Internet communications has made it difficult to separate content from noncontent because “call routing information and content are both contained in the packets.” Taylor, *supra*, ¶ 25. Thus, monitoring Internet communications pursuant to an order permitting a pen register or a trap and trace device is inherently problematic because it is possible for “the government to thereby obtain “‘both call identifying information and call content.’” *Id.* ¶ 25. Such an occurrence is expressly disfavored by 18 U.S.C. § 3121(c), which states that the government should take all technologically reasonable precautions to avoid obtaining call content. As of early 2001, “[t]he breadth of information that the government [could] obtain from Internet networks [pursuant] to the Pen Register [laws was] unclear.” Taylor, *supra*, ¶¶ 7–10.

136. Patriot Act, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288–290 (2001). The words in both the subject line and the body of an e-mail are considered “content” information. FIELD GUIDANCE, *supra* note 134.

137. See FIELD GUIDANCE, *supra* note 134 (stating that, even though no federal court has ever explicitly ruled whether the pen/trap statutes are applicable, “numerous courts . . . have applied the [statutes] to communications on computer networks [anyway]”).

138. For example, many people who use e-mail probably do not use their real names in their e-mail address. Both nicknames and fanciful monikers are common. In contrast, many people who own a telephone are listed by their real name in the telephone book. If the government were monitoring recipients of targeted communications under the new pen/trap laws, and obtained routing information pertaining to both electronic and wire communications, it would take a little more work and authorization to discover the identity of the electronic recipient. Granted, the government might be able to learn something about the content of an e-mail from the subject line, but the government could also guess at the content of a telephone call from knowing the locations of the caller and the callee. Thus, it is possible that using pen/trap authority to ac-

orders in the latter context has been a well-established facet of electronic surveillance law.¹³⁹ Thus, it seems that in enacting this provision of the Patriot Act, Congress was merely updating the pen/trap statutes after becoming aware of how technology had evolved. Also, in a purely procedural sense, this modification improved preexisting law by establishing uniform rules (i.e., rules not dependent on the type of communication device being utilized) for obtaining and using pen/trap orders.

E. Once Obtained, All Pen/Trap Orders Are Now Valid Throughout the United States.

Previously, a pen/trap order was only valid in the district where it was obtained.¹⁴⁰ If the surveillance target moved to a different district, the government had to obtain a second pen/trap order from the new district. The Patriot Act changed this. Now, once a pen/trap order is obtained, it is valid throughout the United States.¹⁴¹

Privacy advocates have criticized this modification, claiming that the change is inconsistent with the Fourth Amendment's requirement that a warrant specify the place to be searched.¹⁴² Even if this were true, it is not clear that a federal district is sufficiently more specific than the entire country. Consequently, the logical conclusion would seem to be that, on this particular measure at least, things are no worse from a privacy perspective after the Patriot Act than they were before it. In addition, this modification does not represent a significant change to the preexisting statutory law. The role of the judge in approving a pen/trap order was always purely ministerial,¹⁴³ and the impact of the modification is solely that it is now procedurally easier for the government to conduct pen/trap surveillance.

quire noncontent information pertaining to e-mail may be less invasive than using the same authority in the traditional manner.

139. See *supra* note 133 and accompanying text.

140. 18 U.S.C. § 3123(a) (2000).

141. Patriot Act § 216, 115 Stat. at 288–90.

142. American Civil Liberties Union, *supra* note 109.

143. See *supra* note 133 and accompanying text.

III. ASSESSING THE THREAT TO PRIVACY

A. *Some Modifications Potentially Threaten Privacy More than Do the Others.*

While each of the Patriot Act modifications discussed in Part II may threaten privacy, not all the potential threats are of equal magnitude. Thus, if the total threat is to be efficiently minimized, it is necessary to be very specific about which modifications pose the greatest threat. Quite simply, some of the Patriot Act modifications are likely to be of little consequence so far as privacy is concerned. For example, Congress's creation of universal pen/trap jurisdiction eliminates what was a purely procedural hurdle. Similarly, Congress's decision to have pen/trap orders apply to both wire and electronic communications formalizes the conclusion already reached by the courts. In effect, Congress merely updated the statute to account for a changing understanding of technology, and these provisions very well could have been enacted even if the September 11 attacks had not occurred.¹⁴⁴ This possibility is less true of the provision that makes it easier to conduct pen/trap surveillance pursuant to FISA. Still, the degree of intrusion is not great enough to warrant serious concern.

Americans, however, should be greatly concerned about the effects of the two remaining provisions. First and foremost, facilitating the use of FISA to circumvent Title III intercept order requirements potentially puts nonterrorists at risk of being investigated and prosecuted as terrorists. Second, allowing roving surveillance to be conducted pursuant to FISA may result in the interception of numerous innocent conversations, many of which will involve U.S. persons.

As a matter of general policy, the problem with these last two modifications is that, even though they probably satisfy Fourth Amendment scrutiny on their face, too much has been left to executive branch discretion.

B. *Americans Have Three Additional Reasons to be Concerned About the Threat to Privacy.*

1. *Synergistic Effects May Be Present.* The common theme that emerges after analyzing each of the modifications discussed in Part II

144. See *supra* Part I.A.

is that the Patriot Act may unnecessarily threaten civil liberties.¹⁴⁵ Almost all of these criticisms reduce to fear that the government will be able to intrude increasingly on the privacy of American citizens. Ultimately, whether the government is unduly intruding is a question of reasonableness. Reasonableness, however, can be an elusive concept,¹⁴⁶ especially because no provision of the Act can be truly evaluated solely on its own merits. It is probable that, when considered en masse, the assorted provisions of the Patriot Act¹⁴⁷ exhibit a synergy that is not otherwise apparent. While such macroanalysis is beyond the scope of this Note, the concerns raised in Parts II and III may be even more valid when they are evaluated as part of the Patriot Act's impact on American society in general.

2. *The Patriot Act Enables Government Agencies to Share Sensitive Information with One Another to a Much Greater Extent than Was Previously Possible.* Any government law enforcement officer or attorney can now disclose the contents of intercepted communications to other federal officers "to the extent that such contents include foreign intelligence . . . information" that will assist the receiving officer "in the performance of . . . official duties."¹⁴⁸ Similarly, any

145. See Electronic Frontier Foundation, *supra* note 116 (stating that the Patriot Act was a "tremendous blow" to the "civil liberties of ordinary Americans"). Some commentators have also expressed concern that antiterrorist zeal, no matter how well intentioned, might impact individuals or activities that are not really terrorist related. See, e.g., Morton H. Halperin, *Protecting Civil Liberties at a Time of Crisis*, Center for Democracy & Technology, at <http://www.cdt.org/security/011025halperin.shtml> (Oct. 25, 2001) (on file with the *Duke Law Journal*) (criticizing the Patriot Act as overly broad).

146. Polls are not necessarily helpful because any data revealed can quickly shift. "After the bombing of the Oklahoma City federal building in 1995," 49 percent of the people polled by one newspaper stated that they thought giving up "some civil liberties [would be necessary] to curb terrorism." Lisa Guernsey, *Living Under an Electronic Eye*, N.Y. TIMES, Sept. 27, 2001, at G1. When the same question was asked in 1997 using the same methodology, "that figure had dropped to 29 percent." *Id.* When the question was again asked shortly after the September 11th attacks, the figure shot up to 79 percent. *Id.* Congressional support is not necessarily revealing either, because sometimes legislators perceive that they cannot afford to oppose certain bills. Regardless, the Patriot Act was passed in the Senate by a vote of 98 to 1 and in the House by a vote of 356 to 66. Clymer, *supra* note 125, at A1.

147. Among other things, the Patriot Act also addresses search and seizure authority, Patriot Act, Pub. L. No. 107-56, § 209-212, 215, 115 Stat. 272, 283-85, 287-88 (2001); money laundering, *id.* §§ 311-330, 115 Stat. at 298-320, and immigration standards. *Id.* §§ 401-428, 115 Stat. at 342-63.

148. Patriot Act, Pub. L. No. 107-56, § 203(b)(1), 115 Stat. 272, 280 (2001); see also *id.* § 905, 115 Stat. at 389 (requiring that, whenever reasonably possible, "the Attorney General . . . shall expeditiously disclose to the Director of Central Intelligence . . . foreign intelligence information acquired by an element of the Department of Justice . . . in the course of a criminal investiga-

foreign intelligence information obtained as part of a criminal investigation, including information obtained as a result of a grand jury proceeding,¹⁴⁹ can also be disclosed under the same conditions.¹⁵⁰ Because the definition of “foreign intelligence information” is sufficiently broad that it encompasses virtually anything that could be construed as a threat to national security, regardless of whether a U.S. person is involved,¹⁵¹ the government can use the Patriot Act to disseminate surveillance information more broadly than it did in the past. Thus, the privacy concerns present may be more significant here than they would otherwise be.

3. *A Recently Publicized Opinion from the FISA Court Disclosed that, Even Before the Patriot Act was Enacted, the Executive Branch Sometimes Failed to Comply with FISA Surveillance Requirements.* In early 2002, the Department of Justice moved the FISA Court to revise the existing FISA minimization procedures, which had been in effect since 1995 and “regulate[d] the acquisition, retention and dissemination of [FISA information].”¹⁵² In particular, the Department requested that the bright line restricting dissemination of FISA information in overlapping intelligence and criminal investigations be eliminated.¹⁵³ Sitting en banc, the judges on the FISA Court

tion.”). Also, “Federal officers who conduct electronic surveillance to acquire foreign intelligence . . . may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against [threats to the national security of the United States].” *Id.* § 504(a), 115 Stat. at 364.

149. *Id.* § 203, 115 Stat. at 280. Disclosure may only occur subject to the conditions set by the court allowing it, and “[w]ithin a reasonable time after such disclosure, an attorney for the government [must] file . . . a notice with the court stating the fact that such information was disclosed and [stating to whom disclosure was made].” *Id.* § 203(a)(V)(ii)–(iii), 115 Stat. at 280. For a discussion of how the Patriot Act impacts grand jury proceedings, see generally Sara Sun Beale & James E. Felman, *The Consequences of Enlisting Federal Grand Juries in the War on Terrorism: Assessing the Patriot Act’s Changes in Grand Jury Secrecy*, 25 HARV. J.L. & PUB. POL’Y 699 (2002).

150. Patriot Act § 203(b)(2)(d), 115 Stat. at 280. The Director of Central Intelligence may “establish requirements and priorities for foreign intelligence information to be collected” pursuant to FISA and may also assist the Attorney General with coordinating the effective dissemination of the information so obtained, but the Director may not “direct, manage, or undertake electronic surveillance . . . operations pursuant to that Act unless otherwise authorized by statute or Executive order.” *Id.* § 901, 115 Stat. at 387.

151. *See id.* § 203(a)(1)(iv), 115 Stat. at 280 (stating that “foreign intelligence information” is information that “relates to the national defense or the security of the United States . . . [or] the conduct of the foreign affairs of the United States”).

152. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, No. 02-429, 2002 WL 1949263, at *3–4 (F.I.S. Ct. May 17, 2002) (en banc).

153. *Id.* at *10.

unanimously rejected the Department's request on the ground that it was "not reasonably designed" to comply with the purpose of FISA.¹⁵⁴ In reaching this conclusion, the FISA Court expressly noted that the Department had failed to comply on numerous past occasions with the minimization procedures then in existence.¹⁵⁵ Consequently, a compelling argument can be made that it would be sensible to err on the side of caution when determining the proper scope of the executive branch's authority to conduct electronic surveillance.

C. The Patriot Act Contains Several Provisions Favorable to Privacy, but These Provisions Are Not Sufficient to Counter the Potential Threat.

Not every aspect of the Patriot Act that pertained to electronic surveillance law impacted privacy negatively. In several instances, just the opposite was true. For example, Congress could have broadened the type of communications subject to CALEA. If it had, communications service providers would have been obligated to ensure that improvements in technology did not interfere with the government's ability to monitor targeted individuals.¹⁵⁶ The Patriot Act, however, imposed no such duty, and so the scope of CALEA remained unchanged.¹⁵⁷

The Patriot Act also protects privacy in that it subjects to disciplinary procedures government officers that improperly disclose sur-

154. *Id.* at *13. The FISA Court rarely sits en banc and renders a decision. Letter from Hon. Colleen Kollar-Kotelly, Presiding Judge, United States Foreign Intelligence Surveillance Court, to Hon. Patrick J. Leahy, Chairman, Committee on the Judiciary, et al., http://www.epic.org/privacy/terrorism/fisa/fisc_ltr_08_2002.html (Aug. 20, 2002) (on file with the *Duke Law Journal*) (noting that the FISA Court had never before "issued an unclassified opinion and order"). Senator Leahy stated that "this ray of sunshine from the judicial branch is a remarkable step forward for constructive oversight." Philip Shenon, *Secret Court Says F.B.I. Aides Misled Judges in 75 Cases*, N.Y. TIMES, Aug. 23, 2002, at A1.

155. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 2002 WL 1949263, at *8 (stating that, "in an alarming number of instances," the results were "troubling"). Specifically, beginning in March of 2000, FISA information was disseminated to law enforcement without the FISA Court's authorization after the FISA Court had expressly instructed the government that the court's authorization was required. *Id.* at *9. Moreover, in September of the same year, the government confessed to misstating and omitting facts on at least seventy-five FISA applications related to the investigation of terrorism. *Id.*

156. *See supra* notes 40-44 and accompanying text.

157. *See* Patriot Act, Pub. L. No. 107-56, § 222, 115 Stat. 272, 292 (2001) ("Nothing in this Act shall impose any additional technical obligation or requirement on a [communications service] provider . . . to furnish facilities or technical assistance.").

veillance information.¹⁵⁸ In addition, an aggrieved person can bring suit against the United States, and, providing that the disclosure was actually improper, the person will receive at least \$10,000 in damages.¹⁵⁹

The Patriot Act also helps computer owners protect themselves against unauthorized trespassers. Before the Patriot bill became law, it was unclear whether the owner of a computer could obtain the assistance of law enforcement in monitoring people that engaged in computer trespassing,¹⁶⁰ and “because [computer owners] often lack[ed] the expertise, equipment, or financial resources required to monitor attacks themselves, they [usually had] no effective way . . . to protect themselves.”¹⁶¹ Now though, computer owners can authorize law enforcement to assist them.¹⁶²

Most significantly, in enacting the Patriot Act, Congress realized that what seemed necessary in the immediate aftermath of September 11 might seem excessive several years later, especially if no further attacks ensued. For this reason, the Patriot Act explicitly provided that some of the electronic surveillance provisions would sunset on December 31, 2005.¹⁶³

While the above provisions protect privacy to a limited extent, they are not capable of countering the threat that the rest of the Patriot Act poses. In particular, the provisions above do nothing to protect the nonterrorist criminal suspect that could, as a result of it now being easier to use FISA to circumvent Title III, potentially be at greater risk of being investigated and prosecuted as a terrorist. Similarly, the provisions discussed above do not reduce the likelihood that innocent citizens will have their real-time conversations intercepted while roving surveillance is being conducted.¹⁶⁴

158. *Id.* § 223, 115 Stat. at 293.

159. *Id.*

160. FIELD GUIDANCE, *supra* note 134.

161. *Id.*

162. Patriot Act § 217, 115 Stat. at 291.

163. *Id.* § 224, 115 Stat. at 295 (stating that, while section 206 (roving surveillance authority for FISA purposes) will sunset, section 203 (information sharing) and section 216 (pen/trap orders) will not).

164. That the roving surveillance provisions will sunset does not help those who may have their innocent conversations intercepted in the meantime.

CONCLUSION

Choices about electronic surveillance have always involved balancing privacy interests with national security concerns. Prior to September 11, there was not really any defining event that caused this country to rethink the balance struck in the 1970s. In some ways at least, it may seem more natural now for Congress to relax the conditions under which electronic surveillance can occur. In other ways though, nothing has changed. Individual liberties still matter. Thus, it is important not to alter the preexisting balance without good cause and to be especially cognizant of privacy concerns when doing so.

The terrorist attacks clearly established sufficient cause, so the question then becomes whether Congress adequately safeguarded privacy to the extent possible. Here, it seems likely that, while most of the modifications will not pose a significant threat, two of them may. Namely, potentially allowing FISA to be used to circumvent Title III intercept order requirements may unnecessarily put nonterrorists at risk of being investigated and prosecuted as terrorists. Similarly, allowing roving surveillance to be conducted pursuant to FISA may result in the interception of numerous innocent conversations, many of which will probably involve innocent American citizens.

The problem with these last two modifications is that, even though they probably satisfy Fourth Amendment scrutiny on their face, too much has been left to executive branch discretion. American history teaches that insufficiently checked executive power to conduct electronic surveillance is dangerous.¹⁶⁵ Thus, where executive power has increased, as it has here, Americans should be concerned that privacy may be unnecessarily threatened as a result. True, the Patriot Act does contain some provisions that protect privacy, but these provisions by themselves are not enough to neutralize the threat. In addition, it is impossible to know the extent to which synergistic effects, the information sharing provisions, or the fact that the executive branch has not always complied with FISA in the past will further impact privacy concerns. As a result, it is all the more important that executive authority be checked to the appropriate degree.

Here, the courts could act as an independent check on executive authority. Specifically, the courts could give substantive meaning to the word “significant” when deciding whether to admit information obtained from FISA surveillance in a criminal proceeding. If the gov-

165. See *supra* Part I.B.1.

ernment were unable to carry the burden of showing that national security had been a “significant purpose” of a FISA investigation, any evidence so tainted could be excluded. In addition, when authorizing roving FISA surveillance, the courts could require the government to report back on a regular basis. That way, the courts would be able to periodically reassess whether roving surveillance was still justified.

Because it does not seem that either of the measures described above would unduly compromise the executive branch’s ability to track suspected terrorists, both measures should be implemented. The rationale for doing so would be that the increased benefit to privacy would far outweigh any additional procedural burden that might be incurred. It would be best if Congress could immediately incorporate these improvements into statutory law. In the meantime, however, the courts should hold that the above suggestions, or else something very similar, are necessarily implied.

Fortunately, the judiciary may already have begun to move in this direction. As discussed earlier, the FISA Court recently rejected the request of the Department of Justice to eliminate the bright line between intelligence gathering and criminal investigation. The FISA Court’s rejection of an overly broad interpretation of the Patriot Act is a good beginning, but that is all it is. Other courts will have to follow where the FISA Court has led. Simply put, the executive’s authority to conduct electronic surveillance cannot be restricted as Congress intended unless the judiciary remains cognizant of the oversight responsibilities with which it has been entrusted.

At the same time, Americans must realize that it would be a mistake to check executive authority too much. Sadly, the world is full of people that despise the United States and the way of life that it represents. As the September 11 attacks demonstrate, some of these people who hate America pose a serious threat, and thus the American government necessarily must have the power to identify, monitor, and bring such people to justice. Nothing in this Note should be interpreted as suggesting that the preexisting law should not have been altered. The nation had been injured, and because the status quo was at least partially to blame, Congress had to make it easier for the government to protect national security. This Note merely seeks to emphasize that, in the context of electronic surveillance, it may be possible to both protect national security and provide greater protection for privacy than currently exists.