Denver Law Review

Volume 80 | Issue 2 Article 4

January 2002

Big Brother at the Door: Balancing National Security with Privacy under the USA Patriot Act

Patricia Mell

Big Brother at the Door: Balancing National Security with Privacy under the USA Patriot Act

BIG BROTHER AT THE DOOR: BALANCING NATIONAL SECURITY WITH PRIVACY UNDER THE USA PATRIOT ACT

PATRICIA MELL†

INTRODUCTION

> *The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he would be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment.*
>
> –from *1984*, by George Orwell, originally published in 1949[1]

In the futuristic world created by George Orwell, there is no personal privacy. Citizens are watched and tracked every minute of the day by the government.[2] They are told that such surveillance is necessary to keep them safe from the enemies of the state.[3] The citizens are led to believe that the uncertainties and insecurities of an open democracy warrants protection of their physical security and freedom from military aggression by the ever present and ever watchful eye of Big Brother—the government.[4] In this futuristic world, homogeneity of thought and action are safe.[5] Divergent views or attitudes are quickly squelched by the government and declared a threat to the security of the state.[6] This futuristic

---

† Professor of Law, Michigan State University – Detroit College of Law; A.B. with Honors, Wellesley College, 1975; J.D., Case Western Reserve University Law School, 1978; Chair, Privacy and Defamation Section, American Association of Law Schools, 2002-2003. The author wishes to express her appreciation to those individuals that gave their assistance, technical and otherwise, to this project. Individuals deserving of special thanks include the author's mother, Thelma W. Mell, a constant source of support and inspiration, and her husband, Dr. Michael Ragland, MD. In addition, thanks are extended to Professor Jose Anderson of the University of Baltimore Law School; Remona Green and Carol Parker, Reference Librarians, Michigan State University – Detroit College of Law; and Aretha Asamoah, the author's research assistant.

1. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 4 (Alfred A. Knopf, Inc. 1992) (1949).
2. *See id.* at 3, 26.
3. *See id.* at 26.
4. *See id.*
5. *See id.*
6. *Id.*

world created by George Orwell has been dismissed by some as "science fiction."[7]

Advances in computer and surveillance technology, as well as the growth of Internet use, have combined to make the constant surveillance of Orwell's novel a possibility. Many street intersections sport video cameras in the attempt to monitor traffic violators.[8] Thermal imaging[9] and spy satellites make it possible to observe the interior happenings of the home. Telephone, e-mail, Internet activity, and all other manners of electronic communication can be monitored.[10] Biometrics methods can be used to identify and track an individual's movement in society.[11] In addition, it has been suggested that a National Identification Card be instituted as a means of monitoring travel patterns.[12] Many of these methods can be used without an individual's knowledge.[13] Today's technology has the potential to eliminate the area in which an individual can legitimately declare privacy from the intrusion of the government. If allowed to do so, the very fabric of our democratic society will change.

---

7. In the 1998 movie *Enemy of the State*, the surveillance techniques of Orwell's world were shown to be science fact. ENEMY OF THE STATE (Touchstone Pictures 1998). In that movie, a "Winston-like" character, played by Will Smith, discovered how little privacy the individual had at the hands of unscrupulous government figures. *Id.*

8. In August 2001, Congress debated the constitutionality of cameras designed to catch traffic offenders. 2001 Burrelle's Information Services, CBS News Transcripts, *CBS Morning News* (CBS television broadcast, Aug. 1, 2001). At that time, only fifty cities in the United States had installed surveillance cameras at traffic intersections. *Id.*

9. *See id.*

10. The Electronic Communications Privacy Act was a 1986 amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which governed wiretaps. *See* 18 U.S.C. §§ 2511–20 (2000). The amendment extended the protections of Title III to the Internet and other digital technologies. *See id.* The following statement appears in the legislative history of the bill:

> If Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment.

Report of the Committee on the Judiciary on the Electronic Communications Privacy Act of 1986, H.R. REP. NO. 647, 99th Cong., 2d Sess. 16-19 (1986).

11. Dana Hawkins, *Body of Evidence*, U.S. NEWS AND WORLD REP., Feb. 18, 2002, at 60.

> The new technologies establish a person's identity based on distinctive physical features. Most include a scanner or camera and software for analyzing the images extracting key features and digitizing the information. The system can then check the digital biometrics against a database to verify identity. Some features such as the iris are distinctive enough to allow a system to pick out one person among millions. Others such as hand proportions are less powerful but still useful for verifying identity.

Id. Each method has benefits and failings. *Id.* The methods include: digital finger scan, hand scan, face scan, iris scan, and signature and voice scan. *Id.*

12. *See* Mike France et al., *Privacy in an Age of Terror*, BUS. WEEK, Nov. 5, 2001, at 82.

13. *See* David Banisar, *Big Brother Goes High-Tech*, COVERT ACTION Q., *available at* http://mediafilter.org/caq/CAQ56brother.html (last visited Nov. 11, 2002).

The United States Constitution does not explicitly guarantee the right to privacy.[14] However, the framers of the Constitution created the Fourth Amendment to be the guardian of American civil liberties.[15] By ensuring freedom from unreasonable governmental intrusion, the Bill of Rights guaranteed core principles.[16] In combination with the First and Fifth Amendments, "the Fourth Amendment safeguard[s] not only privacy and protection against self-incrimination, but [also] conscience and human dignity and freedom of expression as well."[17] Supported by a range of procedural and substantive guidelines, the balance was maintained between the government's authority to regulate activity and the individual's freedom of thought and action.[18]

The weakening of the Fourth Amendment threatens these fundamental values. Unfortunately, recent circumstances have made it neces-

---

14. In addition to the Fourth Amendment, there are several federal statutes that protect the privacy of the individual in specific contexts. These include the Privacy Act of 1974, 5 U.S.C. § 552a (2000) (giving individuals the right to request access to records about themselves and to prevent agency disclosure of personal information to third parties without consent); the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a(o) (2000) (amending the Privacy Act to limit the collection of information from individuals and providing guidelines for matching data about the same individual between agencies); the Privacy Protection Act of 1980, 42 U.S.C. § 2000aa(b) (2000) (establishing guidelines for the police in obtaining information from newspapers); the Right to Financial Privacy Act of 1978 (FPA), 12 U.S.C. §§ 3401-22 (2000) (regulating the manner that the government gains access to bank records about individuals; FPA was amended by the Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act [hereinafter USA PATRIOT Act], Pub. L. No. 107-56, § 505b, 115 Stat. 272, 365 (2001)); the Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232g (2000) (limiting disclosure of student records to third parties without the subject's permission; FERPA was amended by the USA PATRIOT Act, Pub. L. No. 107-56, § 507, 115 Stat. 272, 367); the Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. §§ 1681-1681v (2000) (limiting the disclosure of consumer reports, or investigative consumer reports, to third parties (e.g. government or other users) by consumer reporting agencies; FCRA was also amended by the USA PATRIOT Act, Pub. L. No. 107-56, § 505c, 115 Stat. 272, 365); and the Video Privacy Act, 18 U.S.C. § 2710 (2000) (preventing videotape service providers from disclosing personally identifiable information concerning an individual's tape selection to third parties). For a discussion of these statutes and the nature of the privacy interests protected, see Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight*, 11 BERKELEY TECH. L. J. 1 (1996).

15. "Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.'" United States v. U.S. Dist. Court, E.D. Mich., 407 U.S. 297, 314 (1972).

16. In this article, privacy will be used to describe freedom from governmental intrusion as protected by the Fourth Amendment of the United States Constitution. "[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all." Katz v. United States, 389 U.S. 347, 350 (1967).

17. Frank v. Maryland, 359 U.S. 360, 376 (1959) (Douglas, J., dissenting). The Court, on numerous occasions, has recognized the historical interdependence between the rights that are protected in the First, Fourth, and Fifth Amendments. *See* Stanford v. Texas, 379 U.S. 476, 482-86 (1965); Marcus v. Search Warrants of Property at 104 E. Tenth St., Kansas City, Missouri, 367 U.S. 717, 724-29 (1961); Boyd v. United States, 116 U.S. 616 (1886).

18. *See* discussion *infra* Section I., and text accompanying notes 33-145.

sary for us as a nation to critically assess our resolve to maintain these values. On September 11, 2001, we witnessed in horror the terrorist attacks in New York and Washington, D.C. The crash of the plane in Pennsylvania still causes doubt as to the alleged target. On the ground, in the air, and in the aftermath of these acts, thousands of people lost their lives.[19] Along with the loss in human life, this nation lost its sense of safety and security within its borders.

The government reacted quickly to the crisis with the passage of a comprehensive act designed to assist law enforcement officials in detecting terrorists.[20] The legislation is known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act" or "PATRIOT Act").[21] On October 26, 2001, President George W. Bush signed the PATRIOT Act into law.[22]

The PATRIOT Act is unprecedented in its amendment to provisions that had previously checked the ability of the government to observe everyday activities and obtain personal information about citizens.[23] The

---

19. One year after the terrorist attack, the death toll was reported at 2,823. Brian Reade, *9/11: Stats and Quotes*, THE MIRROR, Sept. 11, 2002.

20. The USA PATRIOT Act was passed within seven weeks of the terrorist attacks. Thomas Legislative Service, *Bill Summary & Status for the 107th Congress*, *at* http:thomas.loc.gov/cgi-bin/bdquery (last visited Feb. 28, 2003). On October 2, 2001, the House introduced H.R. 2975, the Uniting and Strengthening America ("USA Act") Act of 2001. *Id.* The Senate introduced companion anti-terrorism legislation on October 4th—S. 1510, the Uniting and Strengthening ("USA Act") Act of 2001. *Id.* On October 11th, the Senate passed its anti-terrorism bill, followed by House passage of its version on October 12th. On October 23rd, H.R. 3162, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act") was introduced in the House, which incorporated provisions of both the House and Senate passed anti-terrorism bills. *Id.* On October 24th, the USA PATRIOT ACT passed both houses of Congress by an overwhelming majority: in the House by a vote of 357-66, and in the Senate by a vote of 98-1. *Id.* The President signed it into law two days later on October 26th. *Id.*

21. USA PATRIOT Act, Pub. L. No. 107-56, § 1, 115 Stat. 272, 272-75. The 116 pages of the USA PATRIOT Act are divided into ten sections designated as titles. Each title deals with the enhancement of a different set of criminal and civil law enforcement. Title I – Enhancing Domestic Security Against Terrorism; Title II – Enhanced Surveillance Procedures; Title III – International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001; Title IV – Protecting the Border; Title V – Removing Obstacles to Investigating Terrorism; Title VI – Providing for Victims of Terrorism, Public Safety Officers, and Their Families; Title VII – Increased Information Sharing for Critical Infrastructure Protection; Title VIII – Strengthening the Criminal Laws Against Terrorism; Title IX – Improved Intelligence; Title X – Miscellaneous. Despite its title, several of the provisions of the Act are not restricted to curtailing terrorism. Instead, many provisions are permanent changes to the criminal justice system in the United States. *See, e.g.*, USA PATRIOT Act, Pub. L. No. 107-56, § 371c, 115 Stat. 272, 337 (creating a criminal offense called "bulk cash smuggling").

22. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272.

23. The USA PATRIOT Act does make some changes needed to keep law enforcement techniques current with changes in technology; however, these changes have little to do with terrorism. *See id.* § 816, 115 Stat. 272, 385 (establishing cybersecurity forensic training for law enforcement).

fact that it does so in such a potentially oppressive manner has not quite hit the consciousness of the American people.[24] Privacy, in the sense of freedom from governmental intrusion, is a necessary foundation for the free exercise of democracy. However, privacy remains an abstract concept for the majority of Americans.[25]

By contrast, the horror of watching airplanes ramming into the World Trade Center and the Pentagon was concrete. Thus, Americans perceived that drastic measures were needed to prevent new attacks and restore the sense of security rocked by September 11th. The government responded to this perceived need with the PATRIOT Act.[26]

The PATRIOT Act attacks the balance between the government and the individual by a systematic circumvention of established doctrine and procedures guarding against unreasonable governmental intrusion.[27] It expands the realm of foreign surveillance into the domestic arena.[28] It removes many instances of judicial oversight from the system and threatens basic notions of freedom. It supersedes federal privacy protection laws and creates new crimes that may impact the Bill of Rights.[29] In many ways, it has repealed traditional notions of checks and balances between the executive, judicial, and legislative branches of the government.[30] This new standard of executive branch license, combined with a

---

24. Several of the provisions of the Act were challenged by a coalition of right and left wing Congressmen and special interest groups. Attorney General Ashcroft derided them in his testimony before the Senate Judiciary Committee in December 2001. *Dep't of Justice Oversight: Preserving our Freedoms While Defending Against Terrorism: Hearing Before the Sen. Comm. on the Judiciary*, 107th Cong. (2001) (statement of John Ashcroft, Attorney General of the United States). He stated, "to those who scare peace-loving people with phantoms of lost liberty, my message is this: Your tactics only aid terrorists, for they erode our national unity and diminish our resolve. They give ammunition to America's enemies and pause to America's friends." *Id.* The statement has the unfortunate effect of giving credence to civil libertarians who value free speech.

25. Members of various minority groups may disagree, pointing to obsessive use of police power in such things as traffic stops on less than probable cause, i.e. "driving while black." *See* Adero S. Jernigan, *Driving While Black: Racial Profiling in America*, 24 LAW AND PSYCHOL. REV. 127 (2000). Even in these instances, however, there are procedures that redress the government's abuses. *See* State v. Soto, 734 A.2d 350, 352 (N.J. Super. Ct. Law Div. 1996) (granting a motion to suppress evidence seized pursuant to the traffic stops of seventeen African-American males stopped for minor traffic offenses; the court found prima facie evidence of racial discrimination on the part of the state police).

26. The stated purpose of the USA PATRIOT Act is "[t]o deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes." USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (introductory text).

27. *See generally* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272.

28. *See* discussion *infra* note 32 on the Foreign Intelligence Surveillance Act.

29. *See id.*

30. Although expressing some reservations, the pressing nature of the terrorist attacks may have made some members of Congress less willing to object to some of the provisions of the USA PATRIOT Act. Senator Russ Feingold (D-Wis.) was heard to complain that by naming the bill the USA PATRIOT Act, members of Congress were being subtly coerced into voting for it or risk being branded unpatriotic. Heather Forsgren Weaver, *Balance Sways Between Privacy, Security Concerns*, RCR WIRELESS NEWS, Feb. 4, 2002, *available at* http://rcrnews.com/cgi-bin/search.pl.

Fourth Amendment weakened by advances in surveillance technology, could extinguish privacy under the Fourth Amendment and dramatically change the nation.[31]

This article is an assessment of some provisions of the PATRIOT Act and its severe retrenchment of the privacy protected by the Fourth Amendment. It reviews some of the established protections that balanced the government's ability to intrude into the individual's sphere of privacy. This article also compares the traditional distinctions made between the heightened privacy protection standard under the Fourth Amendment for domestic criminal investigations with the lowered standards accepted for investigations performed for the collection of foreign intelligence under the Foreign Intelligence Surveillance Act ("FISA"), which figures so prominently in the PATRIOT Act.[32] Finally, this article examines some provisions of the PATRIOT Act as they impact these privacy protections.

I. THE PRE-PATRIOT ACT SCHEME OF CHECKS AND BALANCES UNDER THE FOURTH AMENDMENT AS PROTECTION OF PRIVACY

A. *The Legitimacy of the Individual's Subjective Expectation of Privacy Under the Fourth Amendment*

> *The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation and particularly describing the place to be searched, and the persons or things to be seized.*[33]

While the Constitution does not specifically designate a right to privacy, the basic purpose of the Fourth Amendment has been to "safeguard the privacy and security of individuals against arbitrary invasions by

---

31. *See generally* ALAN WESTIN, PRIVACY AND FREEDOM (1967). A warning concerning the effects of technology on the Fourth Amendment was given in *Olmstead v. United States*, 277 U.S. 438, 465-66 (1928).

32. The Foreign Intelligence Surveillance Act ("FISA") was enacted to provide guidelines to the Central Intelligence Agency ("CIA") for the collection of intelligence on the activities of foreign powers. 50 U.S.C. §§ 1801-11 (2000). FISA was the Congressional response to a Senate report documenting the flagrant unconstitutional surveillance perpetrated by governmental agencies on domestic organizations critical to the administration. *See* discussion on Church Committee Report, *infra* note 284. Before its amendment by the USA PATRIOT Act, FISA allowed surveillance pursuant to a warrant based on probable cause that the purpose of the surveillance was the gathering of foreign intelligence information. 50 U.S.C. §§ 1804-05. There were very narrowly proscribed circumstances for domestic surveillance. *See* United States v. Squillacote, 221 F.3d 542, 553 (4th Cir. 2000), *cert. denied*, 532 U.S. 971 (2001). Special courts were established to hear applications for FISA surveillance. 50 U.S.C. § 1803.

33. U.S. CONST. amend. IV.

governmental officials."[34] It has balanced the government's exercise of its police power with the individual's right to be free from unreasonable intrusions by the government.[35] The Fourth Amendment did not abolish the government's power to conduct searches of private residences or to seize papers found within. Instead, it imposed a reasonableness requirement upon governmental searches.[36] Requiring a warrant, as a condition precedent to a search, added judicial supervision to the government's exercise of its prerogative to intrude into the individual's private areas.[37] The probable cause standard gave judges a measure by which to decide the appropriateness of the warrant and provided additional insurance that groundless searches would not be allowed.[38]

The framers of the Constitution took great pains to provide a system of checks against governmental action because of their own experiences with the unreasonable and arbitrary searches performed by the English colonial government's officials.[39] Through the writ of a general warrant and writs of assistance, the English government had the power to search *any place* for *any thing*.[40] The use and abuse of such writs by the English militia in colonial America was at the basis of the Fourth Amendment's broad grant of protection to the people.[41]

Both the warrant clause and reasonableness clause of the Fourth Amendment acted as buffers between the government and the individual.[42] However, the Framers did not mean for the individual's privacy to be absolute.[43] The individual's private realm would suffer shifting bor-

---

34. Johnson v. United States, 333 U.S. 10, 14 (1948). *See supra* note 14 for a list of some of the federal statutory protections afforded to individuals.

35. "The Warrant Clause has stood as a barrier against intrusions by officialdom into the privacies of life." United States v. U.S. Dist. Court, E.D. Mich., 407 U.S. 297, 332 (1972) (Douglas, J., concurring).

36. *See* Katz v. United States, 389 U.S. 347, 353 (1967).

37. The requirement that the warrant be issued by a neutral and detached magistrate has its basis in English common law. "[W]here practical, a governmental search and seizure should represent both the efforts of the officer to gather evidence of wrongful acts and the judgment of the magistrate that the collected evidence is sufficient to justify invasion of a citizen's private premises or conversation. Inherent in the concept of a warrant is its issuance by a 'neutral and detached magistrate.'" *U.S. Dist. Court, E.D. Mich.*, 407 U.S. at 316.

38. *See* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 94, 95 n.61 (1937).

39. In Colonial America, the British would search the colonists' homes for evidence of contraband and treason against the crown. *See generally* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.1 (1st ed. 1978).

40. *See* Boyd v. United States, 116 U.S. 616, 622-23 (1886).

41. *See* LASSON, *supra* note 38, at 80; *see also* Entick v. Carrington, 19 Howell's State Trials 1029, 1034 (1765) (describing the search of plaintiff's house under a general warrant).

42. *See* LAFAVE, *supra* note 39, §§ 1.1, 3.1 for a discussion on the operation of these clauses of the Fourth Amendment.

43. *See Katz*, 389 U.S. at 350. It was later suggested that the states might be better able to develop more expansive protections of individual privacy. *See* William J. Brennan, Jr., *State Constitutions and the Protection of Individual Rights*, 90 HARV. L. REV. 489, 490 (1977) ("State

ders as the courts reinterpreted the permissible sphere of privacy before society's varying needs. Advances in technology combined to shrink the shield of the Fourth Amendment as a protector of privacy. With each advance in surveillance technology, the Supreme Court adjusted its analysis to reflect what it considered to be the legitimate sphere of privacy acceptable to society.[44] Determining the appropriate balance between the individual's privacy and the government's power to intrude upon said privacy is one of the most litigated concepts under the Constitution.[45]

B. Surveillance and Fourth Amendment Protection Before the PATRIOT Act

Boyd v. United States[46] was the first case to assess the modern parameters of the Fourth Amendment. It reflected the nineteenth century notion of a very broad sphere of personal privacy.[47] The United States Supreme Court held the manner of intrusion to be irrelevant to the privacy being protected.

> It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, . . . it is the invasion of this sacred right which underlies and constitutes the essence of [the Fourth Amendment].[48]

---

constitutions, too, are a font of individual liberties, their protections often extending beyond those required by the Supreme Court's interpretation of federal law. The legal revolution which has brought federal law to the fore must not be allowed to inhibit the independent protective force of state law—for without it, the full realization of our liberties cannot be guaranteed."); *cf.* Camara v. Mun. Court, 387 U.S. 523, 528 (1967) (upholding a warrantless search by a city building inspector acting under a city ordinance); Tracey Maclin, *Constructing Fourth Amendment Principles from the Government Perspective: Whose Amendment Is It, Anyway?*, 25 AM. CRIM. L. REV. 669, 720, 726 (1988) (discussing whether a warrant requirement would impair the state's "special interests" by interfering with the state's probation system).

44. A thorough review of the changing analysis of Fourth Amendment cases by the Supreme Court is beyond the scope of this article. For that review, see Nadine Strossen, *The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis*, 63 N.Y.U. L. REV. 1173, 1175-76; Silas J. Wassertrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19 (1988).

45. "[I]t is beyond question that the Fourth Amendment has been the subject of more litigation than any other provision in the Bill of Rights. Indeed, I would be willing to wager . . . that . . . lawyers and judges have spilled more words over the Fourth Amendment than all of the rest of the Bill of Rights taken together." LAFAVE, *supra* note 39, at v; *see also* Jeffrey J. Skelton, *Infrared Imaging Technology: Threatening to See Through the Fourth Amendment*, 29 IND. L. REV. 231, 234 n.23 (1995).

46. 116 U.S. 616 (1886).

47. *See* LASSON, *supra* note 38, at 107-10.

48. *Boyd*, 116 U.S. at 630.

Boyd also fixed the outer perimeter of modern Fourth Amendment analysis.[49] It established the principle that the Fourth Amendment applied to "all invasions on the part of the government and its employees [and was not limited to] a man's home, [but encompassed all the] privacies of life."[50] It is not surprising that the broad scope of Fourth Amendment protection granted in *Boyd* was to be restricted in the face of the problems of fighting crime.[51]

Olmstead v. United States[52] was a severe retrenchment of privacy protection under the Fourth Amendment. The case ushered in a balancing approach of individual privacy versus society's need to fight crime using the new technology of wiretaps.[53] In *Olmstead*, the majority determined that the Fourth Amendment protection against governmental intrusion could only be based upon a physical intrusion into the allegedly private space and applied to "material things – the person, the house, his papers, or his effects."[54] Since the wiretap and "capture" of the telephone conversations were not physical evidence, "[t]here was no searching[,] [t]here was no seizure. . . , [t]here was no entry of the houses or offices of the defendants."[55] Thus, the Fourth Amendment did not apply to government wiretaps.

In his dissent, Justice Brandeis predicted the wave of technological advancement and its encroachment upon the individual's right to privacy.[56] As one of the first defenders of the right to privacy, Brandeis viewed the Fourth Amendment as giving citizens protection against

---

49. *See id.* at 622-38; *see also* Agnello v. United States, 269 U.S. 20, 35 (1925) (holding that evidence of unlawful seizure is not admissible); Gouled v. United States, 255 U.S. 298, 309, 311-12 (1921) (holding that property seizure in a lawful manner may be admissible); Silverthorne Lumber Co. v. United States, 251 U.S. 385, 391-92 (1920) (concluding that evidence obtained in an improper way is not admissible and shall not be used); Weeks v. United States, 232 U.S. 383, 393, 398 (1914) (holding that the trial court erred in admitting and using evidence that was illegally obtained by a United States marshal).

50. *Boyd*, 116 U.S. at 630.

51. *See generally* Wayne R. LaFave, *The Present and Future Fourth Amendment*, 1995 U. ILL. L. REV. 111 (1995) (discussing judicial interpretation of the Fourth Amendment by the United States Supreme Court); Note, *Formalism, Legal Realism, and Constitutionally Protected Privacy Under the Fourth and Fifth Amendments*, 90 HARV. L. REV. 945 (1977) (analyzing the broad shifts in legal thought affecting the United States Supreme Court's view on individual rights and how those shifts have affected the Fourth and Fifth Amendments); *The Life and Times of* Boyd v. United States *(1886-1976)*, 76 MICH. L. REV. 184 (1977-78) (discussing changing societal and judicial notions of property and privacy since the United States Supreme Court's landmark decision in *Boyd*).

52. 277 U.S. 438 (1928).

53. *See Olmstead*, 277 U.S. at 455, 464-71.

54. *Id.* at 464.

55. *Id.*

56. *Id.* at 473 (Brandeis, J., dissenting) ("Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.").

every "unjustifiable intrusion by the government . . . , whatever the means employed."[57]

In delivering the majority opinion in *Olmstead*, Justice Taft was not without concern for the protection of the individual's privacy in the face of government surveillance.[58] He suggested that the lack of Fourth Amendment protection could be remedied by legislative enactment.[59] Congress responded with the enactment of the Federal Communications Act.[60]

In the years after *Olmstead*, the privacy protection afforded by the Fourth Amendment continued to narrow. In the 1940s and 1950s, the Supreme Court maintained its restrictive application of Fourth Amendment protection to telephone wiretapping[61] and declined to apply it to a variety of types of government surveillance activities based solely on the lack of a physical intrusion into the area sought to be held private.[62] This physical presence requirement promulgated by the Court and integrated into its Fourth Amendment jurisprudence was laid to rest in *Katz v. United States*.[63]

Katz is important on a number of fronts. Most importantly, it changed the nature of Fourth Amendment analysis from a trespass model to one based on the protection of people, not places.[64] In *Katz*, the defendant was under investigation for violations of a federal statute that pro-

---

57. *Id.* at 478 (Brandeis, J., dissenting). Justice Brandeis was the co-author of one of the first studies of privacy in the modern age. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 220 (1890).

58. *See Olmstead*, 277 U.S. at 465-66.

59. *Id.*

60. In 1934, Congress enacted the Federal Communications Act, formerly Title VI, § 605, 48 Stat. 1103 (codified as amended at 47 U.S.C. § 605 (1969)). Currently, section 605 reads in pertinent part:

> No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person . . . . No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof), or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto.

47 U.S.C. § 605 (2000).

61. *See* Goldman v. United States, 316 U.S. 129, 132-36 (1942).

62. *See id.*; *see also* Clinton v. Virginia, 377 U.S. 158, 158 (1964) (per curiam) (finding listening device implanted into a party-wall did not violate the Fourth Amendment); Silverman v. United States, 365 U.S. 505, 507-08 (1961) (holding § 605 of the Federal Communications Act inapplicable to conversations heard by virtue of a foot long spike mike); Lee v. United States, 343 U.S. 747, 749, 751 (1952) (holding Fourth Amendment inapplicable to conversation from wire placed on the body of an individual).

63. 389 U.S. 347 (1967).

64. *Katz*, 389 U.S. at 351.

hibited knowingly transmitting wagering information in interstate commerce, a domestic crime.[65] A creature of habit, the defendant tended to use a particular public telephone booth to place calls.[66] The police correctly anticipated that the defendant would use the same telephone on a particular day and at a particular time.[67] The government attached an electronic listening and recording device to the outside of the telephone booth, allowing agents to monitor and record the defendant's half of several conversations.[68] These conversations confirmed that he was taking and placing illegal wagers from the telephone.[69] Over the defendant's objection, the government introduced evidence of the telephone conversations at trial.[70]

The government's argument to admit the conversations was based on the trespass model of Fourth Amendment analysis.[71] Pursuant to this view, the interception of the conversation did not constitute a search since a search could only occur if there had been a physical intrusion into a constitutionally protected area.[72] If the Court followed precedent and accepted the government's argument, then the surveillance would have successfully met the constitutional challenge.[73] Instead, the Court repudiated that view and held that the defendant had a justifiable expectation of privacy while using the telephone booth.[74] Consequently, the interception of the conversation constituted a search and seizure within the meaning of the Fourth Amendment and the evidence should be suppressed.[75]

In reaching its determination, the Court returned to the broad, general scope of Fourth Amendment protection developed in *Boyd*. According to the Court,

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[76]

---

65. *Id.* at 354.
66. *Id.*
67. *Id.*
68. *Id.* at 348.
69. *Id.*
70. *Id.*
71. *Id.* at 352-53.
72. *Id.* at 353.
73. *Id.* at 352-53 (citing *Goldman*, 316 U.S. at 134-36 (1942); *Olmstead*, 277 U.S. at 464, 466).
74. *Id.* at 353 ("We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.").
75. *See id.* at 359.
76. *Id.* at 351 (internal citations omitted).

This broader view of privacy did not make the Fourth Amendment into a general constitutional right of privacy.[77] It did, however, reestablish the Fourth Amendment as the individual's guardian against unreasonable government intrusion.

By itself, the majority opinion changed the direction of Fourth Amendment analysis, but it is for Justice Harlan's concurrence that *Katz* is best known.[78] Justice Harlan established the current two-step analysis of Fourth Amendment issues.[79] Under this model, the subject of the search must first have exhibited an actual (subjective) expectation of privacy and, second, the individual's expectation of privacy must be one that society is prepared to recognize as "reasonable."[80] The benchmark of the protection became the sphere of privacy recognized by society as being legitimate under the circumstances.[81] Since *Katz*, the bifurcated inquiry has been used with each new technological advance in surveillance techniques.[82]

A less familiar part of the *Katz* decision foreshadows issues that may arise concerning the government's use of its expanded surveillance powers under the PATRIOT Act—the warrant requirement. After determining that the Fourth Amendment applied to the facts presented in *Katz*, the Court's final issue was whether the search and seizure conducted by the government, without a warrant, complied with constitutional standards.[83] Since the surveillance was conducted without a warrant, it either had to fit one of the exceptions to the warrant requirement or be adjudged unreasonable.[84] The government tried to establish the reasonableness of its surveillance and described the actions of its agents as being very limited in both scope and duration.[85] In fact, on the one occasion

---

77. *Id.* at 350.

78. *See id.* at 360-62 (Harlan, J., concurring).

79. *See id.* (Harlan, J., concurring).

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

81. *See, e.g.*, Veronia School Dist. 47J v. Acton, 515 U.S. 646, 652-53 (1995).

82. The Fourth Amendment has been held to cover searches other than those of homes. Among the government actions deemed to constitute a Fourth Amendment search are: searches conducted of cars, *Carroll v. United States*, 267 U.S. 132, 149 (1925), telephones through the use of listening devices, *Katz v. United States*, 389 U.S. 347, 353 (1967), and other electronic means such as pen registers, *Smith v. Maryland*, 442 U.S. 735, 741-42 (1979), electronic monitoring devices, *United States v. Karo*, 468 U.S. 705, 716 (1985), aerial surveillance, *Dow Chemical Co. v. United States*, 476 U.S. 227, 239 (1986), and thermal imaging devices, *Kyllo v. United States*, 533 U.S. 27, 34-35 (2001). However, the subject of the search was not always successful in asserting Fourth Amendment protection. *See, e.g., Carroll*, 267 U.S. at 162; *Smith*, 442 U.S. at 745-46; *Karo*, 468 U.S. at 706; and *Dow Chemical Co.*, 476 U.S. at 239.

83. *Katz*, 389 U.S. at 354-59.

84. *See id.* at 357 & n.19 ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.").

85. *See id.* at 354.

that the agents intercepted the statements of another person, "the agents refrained from listening to them."[86]

Rather than grant the retroactive validity requested by the government, the Court recognized that the facts supported the conclusion that had a warrant been applied for, it could have been granted by a duly authorized magistrate.[87] The Court decided that a judicial order could have accommodated the legitimate needs of law enforcement by authorizing the carefully limited use of surveillance. Such an order would have protected the individual's privacy by allowing "no greater invasion of privacy than was necessary under the circumstances."[88]

While recognizing that the essence of electronic surveillance rested on a lack of notice to the subject under investigation, the Court refused to create an exception to the warrant requirement for the police.[89]

> Omission of such authorization 'bypasses the safeguards provided by an objective predetermination of probable cause, and substitutes instead the far less reliable procedure of an after the event justification for the . . . search, too likely to be subtly influenced by the familiar shortcomings of hindsight judgment.' And bypassing a neutral predetermination of the scope of a search leaves individuals secure from Fourth Amendment violations 'only in the discretion of the police.'[90]

Notwithstanding the limited nature of the search conducted by the officials in *Katz*, the Court decided that by pursuing the wiretap without first securing a warrant, the government had "ignored the procedure of antecedent justification . . . that is central to the Fourth Amendment, a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case."[91]

Subsequently, the Supreme Court has recognized instances in which a warrant is not a necessary condition precedent to a valid domestic

---

> [The agents] did not begin their electronic surveillance until investigation of the petitioner's activities had established a strong probability that he was using the telephone in question to transmit gambling information to persons in other states in violation of federal law. . . . The agents confined their surveillance to brief periods during which he used the telephone booth, and they took great care to overhear only the conversations of the petitioner himself.

Id.

86. *Id.* at 354 n.15.

87. *Id.* at 356-57.

88. *Id.* at 355-56 (citing Berger v. New York, 388 U.S. 41, 57 (1967)). In an earlier case, the Court had held that an "order authorizing the use of the electronic device in *Osborn* afforded similar protections to those of conventional warrants authorizing the seizure of tangible evidence." *Id.* at 355-56 (citing *Berger*, 388 U.S. at 57) (internal quotations omitted).

89. *Id.* at 358.

90. *Id.* at 358-59 (quoting Beck v. Ohio, 379 U.S. 89, 95, 97 (1964)).

91. *Id.* at 359; *see also* discussion *infra* Section III. and notes 246-403, concerning warrant requirements and surveillance done for the protection of national security.

search.[92] The circumstances include searches incident to arrest,[93] "stop and frisk" searches,[94] automobile searches,[95] searches at immigration ports of entry to the United States,[96] and searches of closed containers in automobiles that have been lawfully stopped.[97]

Since *Katz*, the Court has been consistent in holding that if the government intrusion is a search, the person invoking the protection of the Fourth Amendment will only be successful if he can claim a legitimate and justifiable expectation of privacy from the government's intrusion.[98] As opposed to this precept lending strength to privacy protection under the Fourth Amendment, subsequent cases would constrict the situations in which a justifiable expectation of privacy is found.[99] In many of these

---

92. *See, e.g.*, United States v. Ross, 456 U.S. 798 (1982) (extending the automobile exception to the Fourth Amendment warrant requirement to closed containers found in lawfully stopped and searched vehicles); *see also* Lewis R. Katz, *Criminal Law:* United States v. Ross*: Evolving Standards for Warrantless Searches*, 74 J. CRIM. L. & CRIMINOLOGY 172 (1983) (examining implications to areas relating to the Fourth Amendment after the Supreme Court's decision in *Ross*).

93. *See* United States v. Robinson, 414 U.S. 218, 235 (1973) ("A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification."); Cupp v. Murphy, 412 U.S. 291, 296 (1973) (holding that where police in the course of station-house questioning took samples from the respondent's fingernails there was not an improper search under the Fourth Amendment); Warden v. Hayden, 387 U.S. 294, 298-300 (1967) (explaining exigent circumstances); *see generally Ross*, 456 U.S. 798 (expanding police authority to conduct warrantless searches of automobiles carrying contained containers); Chimel v. California, 395 U.S. 752, 759, 762-63 (1969) (discussing that searches incident to arrest are limited and, when at all possible, police must attempt to obtain judicial approval through warrant procedure).

94. *See* Terry v. Ohio, 392 U.S. 1, 16-31 (1968) (discussing that police officer's conduct of stop and frisk cannot automatically be considered outside the purview of the Fourth Amendment, but rather must be reviewed under a reasonableness standard).

95. Michigan v. Long, 463 U.S. 1032, 1049 (1983); *see also Carroll*, 267 U.S. at 147-49, 151-53 (establishing that contraband goods concealed and illegally transported in an automobile may be searched without a search warrant).

96. *See* United States v. Ramsey, 431 U.S. 606, 616 (1977) (discussing searches upon entering the United States); *see also* United States v. Duncan, 693 F.2d 971, 977-78 (9th Cir. 1982) (discussing searches upon leaving the United States).

97. *See Ross*, 456 U.S. at 798 (finding a warrantless search of closed containers in automobiles valid); *see also* Katz, *supra* note 92, at 172 ("[T]he Supreme Court extended the automobile exception to the Fourth Amendment warrant requirement to closed containers found in lawfully stopped and searched vehicles.").

98. *See* Rakas v. Illinois, 439 U.S. 128, 148 (1978) (holding an automobile has a different expectation of privacy than a dwelling); United States v. Chadwick, 433 U.S. 1, 7 (1977) (ruling the Fourth Amendment protects people from government intrusions into their legitimate expectations of privacy); United States v. Miller, 425 U.S. 435, 442 (1976) (explaining that a court will examine documents to see if contents were within defendant's expectation of privacy); United States v. Dionisio, 410 U.S. 1, 14 (1973) (holding compelled execution of voice and handwriting samples not to be within defendant's expectation of privacy); Couch v. United States, 409 U.S. 322, 335-36 (1973) (ruling no expectation of protected privacy in situation where an accountant is obligated to disclose information); *Terry*, 392 U.S. at 9 ("[W]here an individual may harbor a reasonable expectation of privacy, he is entitled to be free from unreasonable government intrusion.").

99. *See Kyllo*, 533 U.S. at 34 (allowing use of sense-enhancing technology in use generally by the public); *Karo*, 468 U.S. at 712 (holding an unmonitored beeper to not violate anyone's privacy

cases, the governmental intrusion was aided by enhanced surveillance technology.[100] With each new surveillance technique, the Supreme Court attempted to refine the notion of privacy under the Fourth Amendment.[101] As, a result, the parameters of privacy rights that may be protected are in flux. The fluidity of this situation makes the warrant requirement a lynchpin for the protection of privacy.

1. Thermal Imaging[102]

In most cases addressing the use of a "new technology" by law enforcement officers to conduct a search, courts have to consider the question of whether use of the new technology constitutes a search. Initially, the determination of whether the electronic surveillance can be characterized as being a search depends on whether the technology is intrusive into the target area.[103] If the method is not intrusive, it is not a search requiring the protection of the Fourth Amendment and the failure to obtain a warrant will not defeat the use of the evidence found in the target area.[104]

In *United States v. Penny-Feeney*,[105] for instance, a "non-intrusive" Forward Looking Infrared Device ("FLIR") was used in a fly-over of a suspect's residence.[106] An officer used a FLIR to detect the existence of surface waste heat, which can be the incidental by-product of energy sources used to cultivate marijuana.[107] Based on the results from the FLIR flyover, police obtained a search warrant for the defendants' residence.[108] In the search, they discovered evidence of marijuana production.[109] In denying the defendants' motion to suppress, the district court held that the defendants did not manifest an actual expectation of privacy

---

interests); *Smith*, 442 U.S. at 742 (ruling people have no reasonable expectation of privacy when dialing phone numbers); United States v. Penny-Feeney, 773 F. Supp. 220, 226 (D. Haw. 1991) (finding no expectation of privacy in heat voluntarily vented from garage).

100. *See, e.g., Kyllo*, 533 U.S. at 34-35 (using a thermal imaging device to detect heat from heat lamps used to grow marijuana).

101. *See id.* at 34 (allowing use of sense-enhancing technology in use generally by the public); *Karo*, 468 U.S. at 712 (holding an unmonitored beeper to not violate anyone's privacy interests); *Smith*, 442 U.S. at 742 (ruling people have no reasonable expectation of privacy when dialing phone numbers); *Penny-Feeney*, 773 F. Supp. at 226 (finding no expectation of privacy in heat voluntarily vented from garage).

102. "Thermal imaging is a passive, non-intrusive instrument which detects differences in temperature on the surface of objects being observed. It does not send any beams of rays into the area on which it is fixed or in any way penetrate structures within that area." *Penny-Feeney*, 773 F. Supp. at 223.

103. *See Olmstead*, 277 U.S. at 463-64.

104. *See id.* at 464-65.

105. 773 F. Supp. 220.

106. *Id.* at 223-24.

107. *Id.*

108. *Id.* at 224.

109. *Id.*

in the heat waste since they voluntarily vented it outside the garage where it would be exposed to the public and in no way attempted to impede its escape or exercise dominion over it.[110] Likening the heat waste to garbage left on the street, the district court made it clear that even if the defendants had a subjective expectation of privacy, it was not one that society was prepared to recognize as legitimate.[111]

Considering the validity of warrantless thermal imaging surveillance in *Kyllo v. United States*,[112] the Court determined that the use of sense-enhancing technology to gather any information regarding the interior of a home that could not otherwise have been obtained without physical intrusion into constitutionally protected areas constituted a search.[113] The lower courts had held that Kyllo had no subjective expectation of privacy "because he had made no attempt to conceal the heat escaping from his home. . . . [E]ven if he had, there was no objectively reasonable expectation of privacy because the imager did not expose any intimate details of Kyllo's life, only amorphous hotspots on the roof and exterior wall."[114] However, the Supreme Court held that the use of thermal imaging to measure heat emanating from a home was a search, at least where the technology in question was not in general public use.[115] As such, the search was presumptively unreasonable without a warrant.

In making its decision, the Court tried to preserve some measure of privacy against governmental intrusion that existed at the inception of the Fourth Amendment in the eighteenth century.[116] When promulgated, the Fourth Amendment protected the interior of the home.[117] Using that basis, the Court secured for the home a minimal and reasonable expectation of privacy.[118]

> To withdraw protection of this minimal expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. [Thus,] obtaining by sense-enhancing technology any

---

110. *Id.* at 226.

111. *See id.* (citing California v. Greenwood, 486 U.S. 35, 37 (1987)).

112. 533 U.S. 27. *Kyllo*'s facts are substantially similar to those of *Peeny-Feeney*. In *Kyllo*, the police suspected that the target was growing marijuana in his home and used a thermal imaging device to determine if the heat emanating from it was consistent with that which would be created by the high energy lamps required for marijuana growth. *Id.* at 29. The scan did show significantly higher heat emanations coming from the target's home as compared to those of his neighbors. *Id.* at 30. Based in part on the thermal imaging, a judge issued a search warrant for Kyllo's home where agents found marijuana growing. *Id.* Kyllo was indicted on federal drug charges and moved, unsuccessfully, to suppress the seized evidence. *Id.* at 29-30.

113. *Id.* at 40.

114. *Id.* at 31.

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

> information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search--at least where . . . the technology in question is not in general public use.[119]

2. Electronic Beepers[120]

In *United States v. Karo*,[121] the police 'bugged' a can of ether with an electronic beeper and monitored its movement through a series of private houses and privately rented storage facilities without a warrant.[122] Using evidence from both the beeper and actual observation of sites, the police subsequently obtained a search warrant for the target's premises and found cocaine, allowing the suspects to be arrested.[123] The district court granted the defendants' motion to suppress the seized evidence, charging that the initial warrant to install the beeper was invalid.[124] This illegal conduct by the government tainted the resulting seizure.[125]

The Supreme Court decided that the original installation of the beeper did not violate anyone's Fourth Amendment rights, but cautioned against the use of such techniques without a warrant.[126]

> Despite this holding, warrants for the installation and monitoring of a beeper will obviously be desirable since it may be useful, even critical, to monitor the beeper to determine that it is actually located in a place not open to visual surveillance. . . . [S]uch monitoring without a warrant may violate the Fourth Amendment.[127]

The Court then addressed the privacy concerns raised by the monitoring of a beeper in a private residence in a location not open to visual surveillance.[128] The Court determined this to be a violation of the justifiable

---

119. *Id.* at 34 (internal citations omitted).

120. "A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver." *Karo*, 468 U.S. at 707 n.1 (citing United States v. Knotts, 460 U.S. 276, 277 (1983)).

121. 468 U.S. 705. *Karo* is distinguishable from *Knotts* by the fact that although a beeper had been placed in a 5-gallon can of chloroform, the movements of the car and the arrival of the can at the cabin could have been observed by the naked eye. *Id.* at 707. As such, no Fourth Amendment violation was committed by monitoring the beeper during the trip to the cabin. *Id.*

122. *Id.* at 708. Through an informant, police learned that the targets had bought a number of canisters of ether from an informant. *Id.* The ether was to be used to remove cocaine from clothing. *Id.*

123. *Id.* at 710.

124. *Id.*

125. *Id.* The government appealed and the decision was affirmed on slightly different grounds by the court of appeals. *Id.*

126. *Id.* at 713. There was no violation because the informant who consented to the addition of the beeper owned the ether cans. *Id.* at 711.

127. *Id.* at 713 n.3.

128. *Id.* at 714.

interest in privacy held by the members of the residence.[129] "Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."[130] Despite this, the monitoring of the beeper revealed nothing about the contents of the rented locker where the ether was stored and, as such, the use of the beeper was not a search of the locker.[131] The specific locker containing the ether was detected by its distinctive smell,[132] and the police subsequently observed the can of ether being moved from that locker to the home.[133] All of these activities were in plain view and constituted no Fourth Amendment violations.[134] As such, the Court reversed the suppression of the evidence.[135]

3. Aerial Surveillance

The Court has not been willing to extend the individual's legitimate sphere of privacy beyond the confines of the home to include the home's backyard.[136] In *California v. Ciraolo*,[137] the Court determined that a naked eye police inspection of an individual's backyard from a fixed wing aircraft at one thousand feet was not a search.[138] Even though the area was within the curtilage of the home, that fact alone did not bar police observation.[139] Likewise, in *Dow Chemical Company v. United States*,[140] the Supreme Court held that the use of aerial photography to conduct a site inspection under the Clean Air Act was not a search for Fourth Amendment purposes.[141]

As a result of these cases, the individual's sphere of protection from unreasonable governmental intrusion has been progressively whittled

---

129. *Id.*
130. *Id.* at 716.
131. *Id.* at 720.
132. *Id.* at 720-21.
133. *Id.* at 721.
134. *Id.*
135. *Id.*
136. *See* California v. Ciraolo, 476 U.S. 207, 215 (1986).
137. 476 U.S. 207.
138. *Ciraolo*, 476 U.S. at 215 (citing *Dow Chemical Co.*, 476 U.S. at 239); *see also* Florida v. Riley, 488 U.S. 445, 451-52 (1989) (holding that aerial surveillance from a helicopter in public navigable airspace was non-intrusive and did not constitute a search under the Fourth Amendment).
139. *See Ciraolo*, 476 U.S. at 213; *see also* Oliver v. United States, 466 U.S. 170, 181-83 (1984).
140. 476 U.S. 227.
141. *Dow Chemical Co.*, 476 U.S. at 239. The intimate activities associated with family privacy and the home and its curtilage simply do not reach the outdoor areas or spaces between structures and buildings of a manufacturing plant. *Id.* For purposes of aerial surveillance, the open area of an industrial complex is more comparable to an "open field" in which an individual may not legitimately demand privacy. *Id.*

away.[142] It has been diminished even under circumstances in which the subject of the surveillance took steps to secure the area from prying eyes and in situations in which the government used increasingly circumspect methods of surveillance.[143] The juggling of the sphere's parameters has resulted in uncertain standards for the individual's privacy under the Fourth Amendment.[144]

While it may not be clear what the parameters are, the Supreme Court has attempted to fashion protections based upon its sense of the framers' intent. However, the PATRIOT Act has redrawn the lines of the individual's privacy by expanding the type of information susceptible to government acquisition.[145] This expansion reduces the realm in which the individual can have an expectation of privacy under the Fourth Amendment, which impacts other civil liberties.

II. RESTRICTION OF THE LEGITIMATE SPHERE OF PRIVACY BY THE PATRIOT ACT'S AMENDMENT OF PRIVACY PROTECTION LAWS

A. Disclosure of Sensitive Information Under the PATRIOT Act

Current laws shape the parameters of the individual's sphere of privacy by declaring that certain information is not to be disclosed to third parties, including the government, except under specified extraordinary circumstances.[146] The PATRIOT Act makes the disclosure of highly sensitive information routine between a large number of law enforcement agencies and other government personnel.[147] The broad dissemination of information collected for different reasons, some under standards requiring much less than probable cause, could negatively impact the individual's ability to exercise guaranteed civil liberties.

Provisions of the PATRIOT Act eliminate prevailing privacy protection laws, further diminishing the individual's sphere of privacy.[148] Section 505 of the Act amends the Fair Credit Reporting Act,[149] the Financial Right to Privacy Act,[150] and the Electronic Communications Privacy Act,[151] to allow government access to personal information upon

142. *See* LaFave, *supra* note 51, at 121.

143. *See id.* at 112-14.

144. *Id.* at 121. Furthermore, none of the aerial surveillance cases dealt with the propriety of spy satellite surveillance that would be possible for regular law enforcement through the expansion of CIA authority under FISA. *Id.* at 113.

145. USA PATRIOT Act, Pub. L. No. 107-56, § 505, 115 Stat. 272, 365-66 (2001).

146. *See supra* note 14 for a list of federal statutes limiting the disclosure of personal information.

147. USA PATRIOT Act, Pub. L. No. 107-56, § 504, 115 Stat. 272, 364.

148. *See, e.g., id.* § 217, 115 Stat. 272, 291 ("Interception of Computer Trespasser Communications").

149. 15 U.S.C. § 1681u (2000).

150. 12 U.S.C. § 3414(a)(5)(A) (2000).

151. 18 U.S.C. § 2709(b) (2000).

"certification" by an FBI agent that the records are relevant to "an investigation to protect against international terrorism or clandestine intelligence activities."[152] Before the amendment, each of those sections specifically provided government access to the records but, in addition to relevance, also required the government to show that the target of the investigation was "an agent of a foreign power."[153] Section 505 removes the "agent of a foreign power" requirement, and as such, greatly expands government access to a multitude of private records without significant judicial review.[154] In combination with the government's newly enlarged domestic surveillance powers under FISA, Section 505 gives the government unprecedented ability to compile dossiers on private citizens.[155]

In addition to the amendment of these three privacy statutes, the PATRIOT Act also amends the Family Education Rights and Privacy Act ("FERPA")[156] to allow nonconsensual disclosure of student records.[157] FERPA previously limited the disclosure of student records to third parties without the consent of the student or parents.[158] Section 507 amends FERPA to permit access to these educational records in the investigation of domestic or international terrorism, or national security.[159] To secure these records, the government only has to certify that the records are relevant to such an investigation.[160] The application is heard *ex parte*, which precludes the target from contesting disclosure of the information.[161] There is no meaningful review by a court, since the court must issue the order as long as the application contains the certification.[162] Section 507 does say that an investigation of a "United States person" may not be pursued "solely on the basis of activities protected by the First Amendment," but such a statement is not required to be in the certification to the court.[163] Without meaningful judicial oversight, this provision could be used to chill First Amendment speech.

---

152. USA PATRIOT Act, Pub. L. No. 107-56, § 505, 115 Stat. 272, 365.

153. *Id.* §§ 505(a)(2), 505(b), 505(c), 115 Stat. 272, 365 (citing 15 U.S.C. § 1681u, 12 U.S.C. § 3414(a)(5)(A), 18 U.S.C. § 2709(b)).

154. *Id.*

155. *See id.*

156. 20 U.S.C. § 1232g (2000).

157. USA PATRIOT Act, Pub. L. No. 107-56, § 507, 115 Stat. 272, 368 (citing 20 U.S.C. § 1232g).

158. 20 U.S.C § 1232g(a)(1). The records protected include information concerning both students' and parents' finances, confidential letters of recommendation, and students' educational records, including records of students in primary, secondary, and post-secondary educational programs. *Id.*

159. USA PATRIOT Act, Pub. L. No. 107-56, § 507, 115 Stat. 272, 367.

160. *See id.*

161. *See id.*

162. *See id.*

163. *See id.* § 505, 115 Stat. 272, 365.

In several sections, the PATRIOT Act expands the scope of information subject to disclosure to the government.[164] In many instances, these invasions of the individual's privacy are not subject to judicial review.[165]

B. *Expanded Scope of Subpoenas for Records of Electronic Communications*

Section 2703 of Title 18 of the United States Code governs law enforcement's access to records concerning electronic communications services.[166] Under a prior subsection of this provision, a service provider was required to disclose to a government entity "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity and length of service of a subscriber and the types of services the subscriber or customer utilized."[167] Section 210 of the PATRIOT Act removes access to the "the types of services the subscriber utilized," but expands the type of information that a provider must disclose to include "records of sessions times and durations," "any temporarily assigned network address," and any means or source of payment, "including any credit card or bank account number."[168] As opposed to narrowing the scope of information subject to disclosure, the new categories potentially expose more personal information about the target than was previously available.[169] This could have a negative impact on the privacy of all subscribers since it applies to all government investigations, not just investigations of suspected terrorist activity.[170] The potentially negative impact on privacy is compounded by the fact that this broader range of information is available to the government merely through the use of a subpoena.[171]

The PATRIOT Act's reduction of the individual's sphere of privacy makes the requirement of a warrant based on probable cause even more important to the protection of the individual's privacy. Any enactment that increases the scope of information subject to government access, but which reduces judicial oversight of the government's efforts at collection, depresses privacy protection under the Fourth Amendment even further. Several provisions of the PATRIOT Act have that effect by allowing electronic surveillance to be performed by law enforcement

---

164. *See id.* §§ 505, 507, 115 Stat. 272, 365, 367.

165. *See id.*

166. *See* 18 U.S.C. § 2703 (approved Oct. 21, 2002).

167. USA PATRIOT Act, Pub. L. No. 107-56, § 210, 115 Stat. 272, 283 (citing 18 U.S.C. § 2703(c)(2)).

168. *Id.*

169. *See id.*

170. *See id.*

171. *See* 18 U.S.C. § 2703(b)(B)(i); *see also* USA PATRIOT Act, Pub. L. No. 107-56, § 210, 115 Stat. 272, 283.

agencies not subject to the warrant and probable cause requirements under FISA.[172]

C. *Probable Cause as Protection of Privacy*

> *The standard of reasonableness embodied in the Fourth Amendment demands that the showing of justification match the degree of intrusion. By its very nature electronic eavesdropping for a 60-day period, even of a specified office, involves a broad invasion of a constitutionally protected area. Only the most precise and rigorous standard of probable cause should justify an intrusion of this sort.*[173]

Probable cause is the foundation upon which a search warrant may issue.[174] It does not prevent the government from searching private areas; rather, it establishes the constitutional standard that must be met for governmental intrusion to be valid.[175] Probable cause is based upon evidence that establishes more than "a mere suspicion" that a crime is about to be committed by the target of the investigation.[176] It exists where "the facts and circumstances within the officer's knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has or is being committed."[177]

It is not an inflexible rule; it is a "non-technical conception of affording compromise accommodating opposing interests of citizens who are to be safeguarded from unreasonable interferences with privacy and of officers who are charged with enforcing the law."[178] The probable cause required for warrantless searches has fluctuated based upon the perceived intrusiveness of the search, although a uniform standard is viewed as a preferable guide to the police.[179] Due to the highly intrusive

---

172. *See* USA PATRIOT Act, Pub. L. No. 107-56, § 210, 115 Stat. 272, 283; *see also* discussion on FISA *supra* note 32.

173. Berger v. New York, 388 U.S. 41, 69 (1967) (Stewart, J., concurring).

174. *Berger*, 388 U.S. at 49.

175. *Id.* at 64 (citing Warden v. Hayden, 387 U.S. 294, 321 (1967) (Douglas, J., concurring)).

176. Brinegar v. United States, 338 U.S. 160, 175 (1949).

177. *Brinegar*, 338 U.S. at 175-76 (citing Carroll v. United States, 267 U.S. 132, 162 (1925)).

178. *See id.* at 176. In this case, the search was of an automobile moving on a public highway and was made without a warrant by federal officers enforcing the liquor laws. *Id.* at 165. The warrantless search and seizure was the result of months of investigative work in which the targets had offered to sell illicit liquor to undercover police officers. *Id.* at 164. The car and license plate used by the targets had been linked to the targets and they had been observed driving on the most used route for the introduction of illicit liquor in the United States. *Id.* All of these facts constituted the probable cause necessary to stop and search the car without a warrant. *Id.*

179. *See, e.g.*, Camara v. Mun. Court, 387 U.S. 523, 538 (1968) (allowing probable cause to be based upon "reasonable legislative or administrative standards of conducting an area inspection which are satisfied with respect to a particular building"). However, the Court declined to adopt a more extended use of this balancing process. *See* Dunaway v. New York, 442 U.S. 200, 213-14 (1979) ("A single, familiar standard is essential to guide police officers, who have only limited time

nature of electronic surveillance, the probable cause standard should be maintained.[180]

Justice Douglas's concurrence in *Berger v. New York* foreshadowed the adoption of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the extensive probable cause requirements required for electronic surveillance.[181]

> I also join the opinion because it condemns electronic surveillance, for its similarity to the general warrants out of which our Revolution sprang and allows a discreet surveillance only on a showing of 'probable cause.' These safeguards are minimal if we are to live under a regime of wiretapping and other electronic surveillance.
>
> . . . [E]ven though it is limited in time, it is the greatest of all invasions of privacy. It places the government agent in the bedroom, in the business conference, in the social hour, in the lawyer's office--everywhere and anywhere a 'bug' can be placed.[182]

D. The Warrant Requirement as a Protection of Privacy

The warrant requirement is based in the Fourth Amendment as a condition precedent to a lawful search by the government.[183] A variety of statutes established procedural guidelines to law enforcement officials executing warrants to search areas within the individual's putative sphere of privacy.[184] One of the statutory requirements was that prior to the entry of the target's premises, the officer must have given notice to the target of the search, of the officer's authority, and of the purpose to enter the premises.[185] The notice requirement served several purposes, not the least of which was to protect privacy by minimizing the chance of entry of the wrong premises. Even when there was no mistake, notice allowed those within a brief time to prepare for the police entry.[186]

The rule was not inflexible.[187] While it did require federal officers to serve the subject of the search with a copy of the warrant and a receipt

---

and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront.").

180. *See Berger*, 388 U.S. at 62-63.

181. *See id.* at 64-68 (Douglas, J., concurring).

182. *Id.* at 64-65 (Douglas, J., concurring).

183. U.S. CONST. amend. IV.

184. *See, e.g.*, FED. R. CRIM. P. 41 (codified at 18 U.S.C. § 3101 (approved Oct. 11, 2002)).

185. *Id.*

186. LAFAVE, *supra* note 39, at 172. Other purposes include: (i) decreasing the potential for violence, as an unannounced entry could lead an individual to believe his safety was in peril and cause him to take defensive measures; and (ii) preventing the physical destruction of property by giving the occupant an opportunity to admit the officer. *Id.*

187. *See* United States v. Villegas, 899 F.2d 1324, 1336 (2d Cir. 1990) (stating that Rule 41(d) does not impose "an inflexible requirement of prior notice" (citing Katz v. United States, 389 U.S. 347, 355 n.16 (1967)).

that described the material obtained, it did not require that the notice be given before the search took place.[188] This approach recognized that there were circumstances under which prior or even contemporaneous notification to the target of the execution of the search might compromise an ongoing investigation.[189] In those cases, a delayed notice exception was recognized for reasonable cause shown if the officers searched the premises but did not seize any property.[190] The officers then had to demonstrate a good reason for the delay and had to provide the notice within a reasonable period after the search, generally no more than seven days.[191] In addition, if the search took place when the owner of the premises was not present, the owner would receive notice that the premises had been lawfully searched pursuant to a warrant, rather than burglarized.[192] "The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed."[193]

E. The Warrant Requirement and "Sneak and Peek"[194] Authority Under the PATRIOT Act

Section 213 of the PATRIOT Act amends the warrant provisions of 18 U.S.C. § 3103a in several respects.[195] It allows delayed notice for reasonable cause in concert with existing precedent, but allows for the seizure of property for "reasonable necessity," a vague standard under existing law.[196] The most serious problem with section 213, however, is a

---

188. *See* Nordelli v. United States, 24 F.2d 665, 666-67 (9th Cir. 1928).

189. *See Villegas*, 899 F.2d at 1336 (holding that the "Fourth Amendment does not prohibit per se a covert entry performed for the purpose of installing otherwise legal electronic bugging equipment" (citing Dalia v. United States, 441 U.S. 238, 248 (1979))); *see also Katz*, 389 U.S. at 355 n.16 ("[O]fficers need not announce their purpose before conducting an otherwise authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence.").

190. *See Villegas*, 899 F.2d at 1337 (citing *Dalia*, 441 U.S. at 248; *Katz*, 389 U.S. at 355 n.16). Searches without seizures are "less intrusive than a conventional search with physical seizure because the latter deprives the owner not only of privacy but also of the use of his property." *Id.* "The warrant shall be served in the daytime, unless the issuing authority, by appropriate provision in the warrant, and for reasonable cause shown, authorizes its execution at times other than daytime." FED. R. CRIM. P. 41(c)(1).

191. *Villegas*, 899 F.2d at 1337 (citing United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986)).

192. FED. R. CRIM. P. 41(d) (codified at 18 U.S.C. § 3101 (approved Oct. 11, 2002)).

193. *Freitas*, 800 F.2d at 1456.

194. Kevin Corr, *Sneaky But Lawful: The Use of Sneak and Peek Search Warrants*, 43 U. KAN. L. REV. 1103 (1995).

195. USA PATRIOT Act, Pub. L. No. 107-56, § 213, 115 Stat. 272, 286.

196. *See Field Guidance on New Authorities (Redacted) Enacted in 2001, Anti Terrorism Legislation*, at § 213, *available at* http://www.epic.org/privacy/terrorism/DOJ_guidance.pdf (last visited Oct. 28, 2002) (citing *Villegas*, 899 F.2d at 1337; United States v. Ludwig, 902 F. Supp. 121,

reflection of the uncertain meaning of "reasonable period after the search."[197] Recognizing that the requirement of notice within a reasonable period must be based upon the circumstances of each case, the jurisdictions range from seven to forty-five days as being reasonable and therefore constitutional.[198] Some authority suggests that a reasonable period could be even longer.[199]

The PATRIOT Act could have used this opportunity to clarify an existing problem in the law. However, section 213 essentially allows the government to delay the notice indefinitely, since the reasonable post-search notification period may be extended by the court for "good cause shown."[200] This broadening of the exception is not limited to investigations of suspected terrorist activity.[201] The expansion includes searches of areas that contain material constituting evidence of any criminal offenses in violation of the laws of the United States.[202] This provision is not subject to the sunset provision of section 224 and is therefore a permanent feature of the federal criminal code.[203]

F. Pen Registers[204]

A warrant supported by probable cause is generally required when the government intends to intercept the content of the target's messages.[205] When they first became available with ordinary line telephone

---

126 (W.D. Tex. 1995); United States v. Ibarra, 725 F. Supp. 1195, 1200 (D. Wyo. 1989)) [hereinafter *Anti Terrorism Legislation Field Guidance*].

197. *See id.*

198. *Villegas*, 899 F.2d at 1337 (stating that the initial delay should be seven days and only extended with good cause, and relying on the argument that the Constitution itself required prompt notice and that "[s]uch time should not exceed seven days except upon a strong showing of necessity" (citing *Freitas*, 800 F. 2d at 1456)). *But see* United States v. Pangburn, 983 F.2d 449, 454-55 (2d Cir. 1993) (holding that the notice requirement found in Rule 41(d) is not required by the Fourth Amendment and stating that the court, in *Villegas*, did not determine that a warrant was unconstitutional for failure to provide proper notice); United States v. Simons, 206 F. 3d 392, 403 (4th Cir. 2000) (holding that a 45 day delay in notice of execution of warrant does not render search unconstitutional); *see also Anti Terrorism Legislation Field Guidance*, *supra* note 196, § 213.

199. *See Anti Terrorism Legislation Field Guidance*, *supra* note 196, § 209 (citing *Simons*, 206 F.3d at 403).

200. *See id.* (discussing the amendments to 18 U.S.C. §§ 3103(a), 2705, 2510 (2000)).

201. *See id.*

202. *See id.*

203. *See id.*

204. United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977) (stating that Pre-PATRIOT Act, a pen register was defined as "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It did not overhear oral communications and did not indicate whether calls are actually completed."). This was not the content of the conversations themselves. *N.Y. Tel. Co.*, 434 U.S. at 167.

205. *See Berger*, 388 U.S. at 68 (Stewart, J., concurring). The interception of content in messages for extended periods of time is "a broad invasion of a constitutionally protected area. Only the most precise and rigorous standard of probable cause should justify an intrusion of this sort." *Id.* (Stewart, J., concurring). This view is reflected in the elaborate system of probable cause required for wiretaps under Title III. *See id.* at 64-66 (Douglas, J., concurring).

systems, pen registers did not capture content; they only caught the telephone numbers dialed by the target from a particular telephone.[206] For this reason, a court would grant the order to install and use a pen register on the government's certification "that the information [was] likely to be obtained by such installation and use [was] relevant to an ongoing criminal investigation."[207] The statute required the court to issue the order upon seeing the certification and did not permit judicial review of the government's judgment.[208] A judge in the telephone service provider's jurisdiction could issue the order.[209]

In *Smith v. Maryland*,[210] the Supreme Court determined that the individual did not have a legitimate privacy interest in the telephone numbers he dialed.[211] There, the police chose a suspected burglar as a target for surveillance.[212] After the burglary, the target made a series of harassing calls to the victim and drove by her home.[213] Pursuant to her description of the car and man, police spotted the target and recorded his license plate number.[214] After identifying Michael Lee Smith as the registered owner of the car, the police requested that the telephone company "install[] a pen register at its central offices to record the numbers dialed from the telephone in [Smith's] home."[215] The pen register confirmed that Smith had called the victim's telephone number from his home.[216] Admitting the pen register tape into evidence, the trial court convicted Smith, "holding that the warrantless installation of the pen register did not violate the Fourth Amendment."[217]

Despite the fact that Smith used his home telephone, the Supreme Court found that he had "no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'le-

---

206. *See N.Y. Tel. Co.*, 434 U.S. at 161 n.1.

207. 8 U.S.C. § 3123 (2000) (amended 2001). This statute lacks "almost all of the significant privacy protections found in Title III, the statute governing the interception of the actual 'content' of a communication (e.g., a phone conversation or the text of an e-mail message)." Electronic Privacy Info. Ctr., *Analysis of Provisions of the Proposed Anti-Terrorism Act of 2001 Affecting the Privacy of Communications and Personal Information* (Sept. 24, 2001), *at* www.epic.org/privacy/terrorism/ata_analysis.html [hereinafter EPIC].

208. *See* EPIC, *supra* note 207.

209. *See* Computer Crime and Intellectual Prop. Section, 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* (Oct. 2001), *at* http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm [hereinafter *Computer Crime Field Guidance*].

210. 442 U.S. 735 (1979).

211. *Smith*, 442 U.S. at 745.

212. *See id.* at 737.

213. *See id.*

214. *See id.*

215. *Id.*

216. *Id.*

217. *See id.*

gitimate.'"[218] Such an expectation "[was] 'not one that society [was] prepared to recognize as reasonable.'"[219] Consequently, the Court affirmed Smith's conviction.[220]

Traditionally, the Court extended a great deal of protection to activities occurring inside the home.[221] Telephone conversations, regardless of their site of origin, enjoyed a modicum of Fourth Amendment protection.[222] In finding the site of the telephone call immaterial, the Court added limits to the individual's sphere of privacy from electronic telephonic surveillance.[223] Since the pen register did not intercept the content of the conversation, perhaps the Court felt comfortable denying the individual's expectation of privacy, even without the order, based on the relevance standard.

Despite the technological changes in telephony, Congress had not amended the pen register statute since its 1984 enactment. Lower courts compensated for the apparent failing by simply applying the pen register statute to computer communications without legislative guidance.[224] As a result, various parties challenged the application of the statute to "electronic communications based on the statute's telephone-specific language."[225] Under the PATRIOT Act, the recognition of changes in the technology of pen registers and the maintenance of the relevance standard combine to reduce the ability of targets to challenge government overreaching.

G. Pen Registers and Trap and Trace Devices Under the PATRIOT Act

Under section 216 of the PATRIOT Act, the pen register/trap and trace statutes now apply to the collection of "communications on the

---

218. *Id.* at 745.

219. *Id.* at 743 (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)); *cf.* United States v. Miller, 425 U.S. 435, 442-43 (1976) (finding no legitimate expectation of privacy in bank records because they contain information voluntarily exposed to a third party).

220. *Smith*, 442 U.S. at 746.

221. *See, e.g.*, Payton v. New York, 445 U.S. 573, 601 (1980) (emphasizing "the overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic").

222. *See Smith*, 442 U.S. at 746 (Stewart, J., dissenting) ("[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of [the] Fourth Amendment." (quoting United States v. United States Dist. Court, 407 U.S. 297, 313 (1972))).

223. *See id.* at 743. The Court likened the phone numbers dialed by Smith from his home telephone to information voluntarily turned over to a third person. *Id.* at 743-44 (citing *Miller*, 425 U.S. at 442-43; Couch v. United States, 409 U.S. 322, 335-36 (1973); United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963)). Smith assumed the risk that the telephone company could divulge the telephone numbers, and no expectation of privacy could reside with such information. *See Smith*, 442 U.S. at 744.

224. *See Computer Crime Field Guidance*, *supra* note 209.

225. *See id.*

Internet and other computer networks."[226] Accepting that the statute needed an update to reflect current communications practices, the amendments did not take into account how these changes would impact privacy. The Act adds the terms "routing" and "addressing" to the list of items that can be authorized for interception,[227] but does not define them. These terms give rise to privacy concerns because of the peculiarities of Internet operation. Calling a telephone number on an ordinary telephone line reveals little information other than the number itself. When a call goes through a computer, the uniform resource locators ("URLs") carry information about the target beyond a simple address.[228] Pen registers "attached" to computers would inform the observer what Web sites had been visited, "which is like giving law enforcement the power -- based only on its own certification--to require the librarian to report on the books you had perused while visiting the public library."[229] This potentially infringes upon rights guaranteed by the First Amendment.[230] The probable cause standard provides a more appropriate test of the legitimacy of the government's application for disclosure of the information.

Section 216 tries to avoid violations of the individual's privacy by requiring the government to use reasonably available technology "so as not to include the contents of any wire or electronic communications."[231] The statute does allow for the interception of "routing," "addressing," and "signaling." While the government's interpretations of this provision say that this limits the interception to the "To" and "From" information

---

226. *See id.* Section 216 amends 18 U.S.C §§ 3121, 3123, 3124, and 3127. *Id.* This means that these devices can now target such facilities as cellular telephone numbers, specific cellular telephones, Internet user accounts or email addresses, Internet protocol addresses, and port numbers. *Id.* The amendment also allows an applicant for a pen/trap order "to submit a description of the communications to be traced using any of these or other identifiers." *Id.*

227. *See id.*

228. David W. Baker, *A Guide to URLs*, *at* http://www.netspace.org/users/dwb/url-guide.html#what (last visited Mar. 12, 2003). Unlike a telephone number,

> [a] URL is like your complete mailing address: it specifies all the information necessary for someone to address an envelope to you. However, they are much more than that, since URLs can refer to a variety of very different types of resources. A more fitting analogy would be a system for specifying your mailing address, your phone number, or the location of the book you just read from the public library, all in the same format.

Id. In June 2000, the FBI advised Senator Leahy, Chairman of the Senate Judiciary Committee, that pen register devices "capture all electronic impulses transmitted by the facility on which they are attached, including such impulses transmitted after a phone call is connected to the called party." *See* 147 CONG. REC. S10990-02 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy). "The impulses made after the call is connected could reflect the electronic banking transactions a caller makes . . . or the electronic ordering of a prescription drug." *Id.*

229. Am. Civil Liberties Union, *USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances, An ACLU Legislative Analysis*, *at* http://archive.aclu.org-/congress/l110101a.html (last visited Mar. 2, 2002).

230. *See* Am. Library Ass'n, *Library Community Statement on Proposed Anti-terrorism Measures*, *at* http://www.ala.org/washoff/terrorism.pdf (last visited Oct. 14, 2002).

231. USA PATRIOT Act, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288.

contained in an e-mail header,[232] the e-mail header also includes the "subject line," which could be considered to be content.

The courts must clarify this contradiction. In essence, section 216 allows for the collection of personal information without the privacy protection provided by the judicial probable cause review under the established wiretap law. It retains this provision's relaxed standard of relevance, expanding the scope of potentially discoverable private information. Section 216 exacerbates this lowered standard of legitimacy by authorizing pen register/trap and trace orders with nationwide effect.[233]

The practical realities of multi-jurisdictional Internet communications make it clear why the government would want this ability in its arsenal. An order for this type of surveillance could previously be granted only "within the jurisdiction of the court."[234] A single communication could pass through several different carriers in a range of jurisdictions.[235] In order to follow the communication to its source, prior law required that the government seek the support of a prosecutor in each successive jurisdiction to obtain an order in that jurisdiction.[236] This slowed down the investigation.[237]

The government's practical solution imposes a burden on any carrier seeking to challenge the installation of the pen register/trap and trace device for legal or procedural defects. Section 216 removes another legal safeguard from the system by requiring carriers to travel to the distant court that issued the order. [238] "The burden would be particularly acute for smaller providers -- precisely those, for instance, who are most likely (according to the FBI) to be served with orders requiring the installation of the Carnivore system."[239]

The expansion of Pen Registers and Trap and Trace devices to the Internet opens the door to the FBI's use of Carnivore without significant court review.[240] Carnivore raises controversial issues because it "pro-

---

232. Leonard Bailey, *Computer Crimes and Intellectual Property Section Department of Justice, International Terrorism, the Internet, and the USA Patriot Act, at* www.usdoj.gov/usao-/eousa/foia_reading_room/usab5003.pdf (last visited Mar. 10, 2003).

233. *See id.*

234. *See Computer Crime Field Guidance, supra* note 209.

235. *See id.*

236. *See id.*

237. *See id.*

238. *See* EPIC, *supra* note 207.

239. *Id.*

240. According to the FBI:

> The Carnivore device provides the FBI with a "surgical" ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept. . . . The Carnivore device works much like commercial "sniffers" and other network diagnostic tools used by ISPs every day, except that it provides the FBI with a unique ability to distinguish between communications which may be lawfully intercepted and those which may not. For

vides the FBI with access to the communications of all subscribers of a monitored Internet Service provider [("ISP"),] . . . not just those of the court-designated target."[241] Section 216 provides that if the communications provider cannot carry out the court order, the government may install a device of its own.[242]

Essentially, Section 216 allows the judge, operating under a relevance standard, to issue a blank warrant to a succession of communications carriers.[243] This fails to meet the Fourth Amendment requirement of specifying the place to be searched.[244] It also deprives the judge of the ability to monitor the extent to which government officials utilize the order to access information about Internet communications.[245]

Section 216 expands the scope of information subject to government surveillance, but does not provide any of the privacy protections of prior law. It also allows access to items containing content without any independent judicial review. These provisions, as well as the nationwide service, all reduce the individual's privacy from governmental intrusion. This impacts both Fourth Amendment protections and First Amendment rights. Since Congress did not subject Section 216 to the sunset provisions of Section 224 of the PATRIOT Act, it represents a permanent change to the federal criminal code.

> example, if a court order provides for the lawful interception of one type of communication (e.g., e-mail), but excludes all other communications (e.g., online shopping) the Carnivore tool can be configured to intercept only those e-mails being transmitted either to or from the named subject.

Federal Bureau of Investigation, *Carnivore Diagnostic Tool, at* www.fbi.gov.hq/lab/carnivore/carnivore2.htm (last visited Mar. 1, 2002).

241. EPIC, *supra* note 207. In response to the FBI's introduction of Carnivore in July 2000, some members of Congress expressed their "intent to examine the issues and draft appropriate legislation." *Id.*

242. *See* USA PATRIOT Act, Pub. L. No. 107-56, § 216, 115 Stat. 272, 289. Under these circumstances,

> [s]ection 216 require[s] the law enforcement agency to provide the following information to the court under seal within 30 days: (1) the identity of the officers who installed or accessed the device; (2) the date and time the device was installed, accessed, and uninstalled; (3) the configuration of the device at installation and any modifications to that configuration; and (4) information collected by the device.

See Computer Crime Field Guidance, *supra* note 209. The government may use devices such as Etherpeek or DCS 1000 (a.k.a. Carnivore). *See id.*

243. The section does require that the issuing court have jurisdiction over the particular crime being investigated. *See* USA PATRIOT Act, Pub. L. No. 107-56, § 216, 115 Stat. 272, 290.

244. The Fourth Amendment provides in pertinent part, "[N]o Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

245. The certification of probable cause by a neutral magistrate protects the privacy of the subject of a proposed search from the over-zealousness of the police in their attempt to discover evidence of a crime. *See generally* Aguilar v. Texas, 378 U.S. 108 (1964) (discussing the importance of the magistrate's informed decisions on probable cause); Johnson v. United States, 333 U.S. 10 (1948) (discussing the warrant as a guard against governmental eagerness to search apparently private areas).

III. THE PRIVACY IMPLICATIONS OF THE EXPANSION OF FISA TO DOMESTIC INVESTIGATIONS

Law enforcement officials often pursue intelligence surveillance by the use of wiretapping technologies. Consequently, the PATRIOT Act closely links the federal wiretapping statute and the Foreign Intelligence Surveillance Act ("FISA"). The divergent histories of these two statutes provide the most compelling arguments for retracting the extensive grants of authority given to the executive branch under the PATRIOT Act. Without the reestablishment of traditional checks and balances on the government's ability to conduct domestic clandestine surveillance, the history of the government's flagrant violations of the individual's exercise of First Amendment freedom could become this nation's prologue.

A. *Intelligence Surveillance and Wiretapping*

> *History abundantly documents the tendency of Government – however benevolent and benign its motives – to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs.*
>
> *The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.*[246]

Through its interpretation of the Fourth Amendment, the Supreme Court has narrowed the legitimate sphere of the individual's privacy in the attempt to balance the government's need to regulate activity and the citizens' right to live free from government involvement.[247] The inevitable conflict between these two imperatives becomes tenser when the government performs surveillance to protect national security.[248] In its amendments to FISA, the PATRIOT Act abandons a long held taboo and extends domestic surveillance authority to the Central Intelligence

---

246. United States v. United States Dist. Court, 407 U.S. 297, 314 (1972).

247. While the Fourth Amendment "protects . . . against certain kinds of governmental intrusion, . . . its protections go further, and often have nothing to do with privacy at all," while other aspects of privacy are protected by different provisions of the Constitution or left to state law. *See* Katz v. United States, 389 U.S 347, 350-51 (1967).

248. *See infra* text accompanying notes 292-301 concerning the prior restraints on foreign intelligence surveillance under FISA. *See generally* William F. Brown & Americo R. Cinquegrana, *Warrantless Physical Searches For Foreign Intelligence Purposes, Executive Order 12,333 and The Fourth Amendment*, 35 CATH. U. L. REV. 97 (1985) (describing the use of warrantless physical searches, and judicial exceptions and parameters for intelligence gathering).

Agency ("CIA").[249] This action eliminates a long recognized distinction between acceptable warrantless electronic surveillance performed in the name of national security and surveillance supported by probable cause necessary for the prosecution of ordinary criminal matters.[250]

Governmental surveillance for the protection of national security emphasizes the interdependency of the First Amendment's freedom of speech and of association and the Fourth Amendment's freedom from unreasonable governmental intrusion.[251] Neither value can "exist without the other."[252] Abuse of the governmental prerogative to institute surveillance without judicial oversight has been demonstrated to negatively impact the other freedoms guaranteed by the Constitution.[253]

B. The Traditional Prohibition of Domestic Authority for Intelligence Collection

The government has used clandestine electronic surveillance devices for many years.[254] *Olmstead v. United States*[255] supported the use of these techniques by excluding governmental wiretapping from the ambit of the Fourth Amendment.[256] Enacted shortly after the *Olmstead* decision, the Federal Communications Act ("FCA") of 1934 protected citizens from the unauthorized disclosure of information obtained through electronic surveillance and from the use of the fruits of government wiretaps.[257] It did not, however, stop the practice of clandestine surveillance.

Despite the enactment of the FCA, the government continued to employ warrantless electronic surveillance in cases involving national security or threats to human life.[258] Congress perceived this ability as so threatening to democracy that it limited the CIA to the investigation of

---

249. USA PATRIOT Act, Pub. L. No. 107-56, § 901, 115 Stat. 272, 387 (2001).

250. Aware of the potential for abuse, Congress "was unwilling to make [the CIA] a policeman at home, or to create conflict between the CIA and the FBI." Weissman v. CIA, 565 F. 2d 692, 695 (D.C. Cir. 1977); *see generally* Sherri J. Conrad, *Executive Order 12,333: Unleashing The CIA Violates the Leash Law*, 70 CORNELL L. REV. 968 (1985).

251. *See* RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS 193 (West 1999).

252. *Id.* at 194.

253. *See id.*

254. *See Intelligence Activities: The National Security Agency and Fourth Amendment Rights, Hearing Before the Senate Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 84, 87 (1975) (statement of Att'y Gen. Edward H. Levi) [hereinafter *Intelligence Activities*]; Note, *The Foreign Intelligence Surveillance Act: Legislating a Judicial Role in National Security Surveillance*, 78 MICH. L. REV. 1116, 1116 (1980).

255. 277 U.S. 438 (1928), *overruled in part by* Berger v. New York, 388 U.S. 41 (1967) and *Katz*, 389 U.S. 347.

256. *See Olmstead*, 277 U.S. at 466.

257. *See* Nardone v. United States, 302 U.S. 379, 380-82 (1937).

258. *Intelligence Activities*, *supra* note 254, at 85-87.

non-domestic issues.[259] Congress later construed this to mean that the CIA could also conduct clandestine intelligence gathering and surveillance abroad.[260]

From the beginning, congressional leaders recognized the potential for abuse by an organization with authority to pursue clandestine surveillance.

> [The C]entral [I]ntelligence agency is supposed to collect military intelligence abroad: but we want to be sure it cannot strike down into the lives of our own people here. So we put in a provision that the agency shall have no police, subp[o]ena, law–enforcement powers, or internal–security functions.[261]

Congress, therefore, limited the CIA's activities to foreign intelligence gathering because of the potential for abuse inherent in making the CIA "a policeman at home."[262] Administration officials reemphasized the primacy of the law barring the CIA from domestic intelligence collection activities.[263]

In *Weisman v. CIA*, the District of Columbia Circuit Court of Appeals stated that the National Security Act of 1947 "was intended, at the very least, to prohibit the CIA from conducting secret investigations of United States citizens, in this country, who have no connection with the Agency."[264] The court noted:

---

259. The CIA succeeded the Office of Strategic services ("OSS"), which President Roosevelt created to gather and analyze wartime strategic information. COMM'N ON CIA ACTIVITIES WITHIN THE UNITED STATES, REPORT TO THE PRESIDENT 45 (1975) [hereinafter ROCKEFELLER COMMISSION]; *see generally* H. RANSOM, THE INTELLIGENCE ESTABLISHMENT (1970). Disbanded in 1945, the OSS had no domestic surveillance authority. ROCKEFELLER COMMISSION, *supra*, at 46. Two years later, President Truman created the Central Intelligence Group ("CIG") to operate abroad. *See generally* Michael Warner, *Salvage and Liquidate: the Creation of the Central Intelligence Agency*, *at* http://www.cia.gov/csi/studies/96unclass/salvage.htm (last visited Mar. 24, 2003). Finally, the National Security Act of 1947 replaced the CIG with the CIA and again restricted the agency's activities to overseas intelligence activities. National Security Act of 1947, Pub. L. No. 80-253, § 102, 61 Stat. 495, 498 (1947).

260. S. REP. NO. 94-755, bk.1, at 128 (1976).

261. Conrad, *supra* note 250, at 974-75 (alteration in original).

262. *Weissman*, 565 F.2d at 695.

263. *See* Conrad, *supra* note 250, at 975. In 1947, Central Intelligence Group Director Vandenberg told Congress that the "prohibition against police powers or internal security functions will assure that the Central Intelligence Group [predecessor of Central Intelligence Agency] can never become a Gestapo or Security Police." *Id.* (quoting *Hearing on S. 758 Before the Senate Comm. on Armed Services*, 80th Cong. 497 (1947) (statement of Hoyt S. Vandenberg, Director, Central Intelligence Group)). Dr. Vannevar Bush echoed this theme when he testified before Congress that the CIA posed "no danger" of becoming a Gestapo because "the bill provides clearly that it is . . . not concerned with intelligence on internal affairs." *See National Security Act of 1947: Hearings on H.R. 2319 Before the House Comm. on Expenditures in the Exec. Departments*, 80th Cong. 559 (1947) (testimony of Dr. Vannevar Bush, Chairman, Joint Research and Development Board, War and Navy Departments).

264. *Weissman*, 565 F.2d at 695.

> Congress wisely sought from the outset to make sure that when it released the CIA genie from the lamp, the Agency would be prevented from using its enormous resources and broad delegation of power to place United States citizens living at home under surveillance and scrutiny. It denied the Agency police or internal-security functions to obviate the possibility that overzealous representatives of the CIA might pry into the lives and thoughts of citizens whose conduct or words might seem unconventional or subversive.[265]

When an investigation targeted "an agent of a foreign power," however, the intelligence community continued to pursue warrantless surveillance on the assumption that an exemption to the Fourth Amendment warrant requirement authorized such activity.[266]

The Supreme Court reserved judgment on the issue as it related to national security, but the justices did not unanimously support that position. In a footnote to the *Katz* decision, the majority stated that they had not been asked to determine "whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security."[267] The Court inferred that in matters of national security, the executive branch's determination of necessity would alleviate the need for government agents to comply with the warrant clause of the Fourth Amendment.[268]

Granting such deference to the executive branch prompted a concurring opinion from Justice Douglas. Justice Douglas decried it as a "wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels 'national security' matters."[269] Justice Douglas observed that in matters of national security the President and the Attorney General could not be "neutral and disinterested," but rather they must act as interested parties—adversaries protecting the nation's interests.[270] If the executive branch tried to simultaneously wear both hats, Douglas speculated that the individual's freedom, as protected by the Fourth Amendment, would suffer.[271]

---

265. *Id.*; *see also* Birnbaum v. United States, 588 F.2d 319, 329-32 (2d Cir. 1978) (discussing the authority of the CIA).

266. *See* Conrad, *supra* note 250, at 979; *see generally* David S. Eggert, Note, *Executive Order 12,333: An Assessment of the Validity of Warrantless National Security Searches*, 1983 DUKE L.J. 611 (1983) (arguing the national security exception to the Fourth Amendment warrant requirement is unconstitutional).

267. *Katz*, 389 U.S. at 358 n.23.

268. It is peculiar that the Court would make such a statement outside of the issues raised. It could be that the Court made the statement in reference to Congressional discussion of the Omnibus Crime Control and Safe Streets Act of 1968, enacted the following year.

269. *Katz*, 389 U.S. at 359 (Douglas, J., concurring).

270. *See id.* at 359-60 (Douglas, J., concurring).

271. *See id.* at 360 (Douglas, J., concurring).

> Since spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers . . . , I cannot agree that where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured where the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate.[272]

Justice Douglas observed that the framers of the Constitution did not distinguish between types of crimes in considering the application of the Fourth Amendment protections from unreasonable search and seizure.[273] As such, the judiciary should maintain its oversight of the executive branch's exercise of surveillance, even under circumstances of national emergency. The rules should "not [be] improvise[d] because a particular crime seems particularly heinous."[274]

Likewise, in *United States v. United States District Court*, the Court declined to address whether the Fourth Amendment applied to foreign intelligence surveillance.[275] It also rejected the government's claim of a national security exemption from the Fourth Amendment for domestic matters because of the impact such license could have on civil liberties.[276]

The PATRIOT Act's creation of the crimes of "domestic terrorism" and "harboring a terrorist"[277] could negatively impact the exercise of unpopular political ideas, just as the Court warned in these prior cases. Section 802 of the PATRIOT Act defines domestic terrorism as activities that:

> (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
>
> (B) appear to be intended—
>
> (i) to intimidate or coerce a civilian population;
>
> (ii) to influence the policy of a government by intimidation or coercion; or
>
> (iii) affect the conduct of a government by mass destruction, assassination or kidnapping; and

---

272. *Id.* (Douglas, J., concurring).

273. *See id.* (Douglas, J., concurring). Here, Justice Douglas noted that Article III, section 3 of the U.S. Constitution gave treason a limited definition, but it did not receive special status under the Fourth Amendment. *Id.* (Douglas, J., concurring).

274. *Id.* (Douglas, J., concurring).

275. *United States Dist. Court*, 407 U.S. at 321-22 ("We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents.").

276. *See id.* at 320.

277. USA PATRIOT Act, Pub. L. No. 107-56, §§ 802-03, 115 Stat. 272, 376.

(C) occur primarily within the territorial jurisdiction of the United States.[278]

Section 803 of the PATRIOT Act makes the act of harboring or concealing any person known or reasonably believed to have committed one of several named offenses a crime punishable by fine, imprisonment, or both.[279] If section 802 clearly defined the crime of domestic terrorism, section 803 would be less problematic. Section 802, however, could be subject to constitutional challenge as being both vague and overbroad. Under the language of section 803, the government could classify as domestic terrorism any activity it found unpopular, including such legitimate activist actions as labor union strikes and protests concerning abortion rights, animal rights, civil rights, the environment, or the G-4. A comprehensive provision such as section 803 invites government overreaching.

Protests that arouse the emotions of a large crowd could become dangerous to human life. By their terms, protests intend to "intimidate or coerce a civilian population" and/or to "influence the policy of a government."[280] The government may also disfavor protests challenging its policies. Provisions such as sections 802 and 803 could make any such group or participating individual a target of governmental surveillance.

Unfortunately, this concern is not a speculative one. Less than 30 years ago, the government of the United States was found by a Senate committee to have violated the civil liberties of American citizens who challenged governmental policies.[281] In one case, the government repeatedly conducted warrantless electronic surveillance of an organization's lawful contacts with citizens of Soviet Russia.[282] Attorney John Mitchell authorized several surveillance requests to provide the FBI with advance knowledge of any activities that could cause international embarrassment

---

278. *Id.* § 802, 115 Stat. 272, 375. "International Terrorism" is defined, in part, as "activities that . . . occur primarily outside the territorial jurisdiction of the United States." 18 U.S.C. § 2331(1) (2000).

279. USA PATRIOT Act, Pub. L. No. 107-56, § 803, 115 Stat. 272, 376-77.

280. *Id.* § 802, 115 Stat. 272, 375.

281. In 1975, the United States Senate established a committee to "conduct an investigation of governmental operations with respect to intelligence activities and the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency of the Federal Government." S. Res. 21, 94th Cong. § 1 (1975). Under the leadership of Sen. Frank Church, the Committee made the following statement in its report: "The Committee's investigation has, . . . confirmed substantial wrongdoing. And it had demonstrated that intelligence activities have not generally been governed and controlled in accord with the fundamental principles of our constitutional system of government." S. REP. NO. 94-755 (1976). "United States intelligence agencies have investigated a vast number of American citizens and domestic organizations. FBI headquarters alone has developed over 500,000 domestic intelligence files." *Id.* at 6.

282. *See* Zweibon v. Mitchell, 516 F.2d 594, 608-10 (D.C. Cir. 1975). The Jewish Defense League contacted Soviet citizens concerning that country's restrictive emigration policies. *Id.*

to the United States.[283] Several other vast investigations occurred even when the citizens concerned had no ties to foreign powers.[284]

In several instances, the government used collected information to actively disrupt protest organizations.[285] To discredit the leaders of activist organizations, the government selectively leaked negative information about the individuals to third parties.[286] Through its COINTELPRO program, the FBI selectively shared "information from its investigations to deny people employment and to smear their reputations."[287] The Church Committee Report documented the FBI's attempt to discredit Dr. Martin Luther King.[288] The FBI justified its continued political surveillance of Dr. King by saying "that some of [his] advisors were Communists," i.e., a threat to national security.[289] It then disclosed derogatory information about Dr. King to the "media and other private organizations" in an effort to block his selection as a recipient of the Nobel Peace Prize.[290] The FBI also resorted to the intimidation and harassment of Dr. King. In one instance, the FBI sent a prepared composite tape recording to Dr. King apparently inviting him to commit suicide.[291] The government took these actions under a system that provided little or no oversight of its intelligence collection activities.

---

283. *Id.* at 610.

284. Due to allegations of improper surveillance, President Ford formed the Commission on CIA Activities Within the United States under the leadership of then Vice President Rockefeller. *See* Exec. Order No. 11,828, 40 Fed. Reg. 1219 (1975). The Commission's investigation confirmed that the Agency collected information on several individuals, many of whom were civil rights and anti-war activists. ROCKEFELLER COMMISSION, *supra* note 259. The Agency had intercepted, opened, and photographed first class letters, and indexed and computerized the names of alleged domestic political dissidents. *Id.* The Church Committee Report described how Project MERRIMAC "expanded into a general collection effort whose results were made available to other components in the CIA, and . . . the FBI." *See* S. REP. NO. 94-755, at 725 (1976).

285. 147 CONG. REC. S10990-02 (daily ed. Oct. 25, 2001).

286. *See id.*

287. *Id.*

> Beginning with Communist and socialist groups, the FBI's COINTELPRO operations spread in the 1960s to the Klan, the "new left," and black militants. Elements of the civil rights and antiwar movements were targeted for disruption because of suspicion that they were "influenced" by communists; others because of their strident rhetoric. When some targets were suspected of engaging in violence, the FBI's tactics went so far as to place lives in jeopardy by passing false allegations that individuals were government informants.

Id.

288. *See* S. REP. NO. 94-755, at 11 (1976).

289. 147 CONG. REC. S10990-02, S10993 (daily ed. Oct. 25, 2001).

290. *Id.*

291. *Id.*

C. *Intelligence Surveillance Under FISA*[292]

Concerns over the domestic abuse of surveillance gave rise to FISA, which instituted a set of procedures for the electronic collection of foreign intelligence and counterintelligence.[293] Significantly, FISA allowed the government a higher degree of governmental intrusion with a significantly lowered standard of review in certain instances when seeking foreign intelligence information.[294] When applying for an order, FISA required the government to identify the target of the surveillance, list the information relied on by the government to demonstrate that the target represented "a foreign power or an agent of a foreign power," and certify that the order sought to obtain "foreign intelligence information."[295] FISA's provisions established a scheme of surveillance oversight that purportedly protected the individual's privacy.[296]

Since the government could authorize foreign intelligence surveillance under less than a probable cause standard, the government could use it at trial only with the Attorney General's advance authorization and after giving notice to the "aggrieved person."[297] This notice gave rise to the aggrieved person's opportunity to suppress the information based on the illegality of the surveillance.[298] However, reviewing courts consid-

---

292. Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978).

293. *See* S. REP. NO. 95-701, at 5 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3974.

294. *See* Foreign Intelligence Surveillance Act ("FISA") of 1978, Pub. L. No. 95-511, § 102, 92 Stat. 1783, 1786. Otherwise, FISA maintains the requirement of a court order authorizing foreign intelligence electronic surveillance. The order requirements under FISA are similar to those for obtaining an order under Title III. After obtaining the Attorney General's approval, the federal officer must make application for the order to one of seven U.S. Foreign Intelligence Surveillance Court ("USFISC") judges. *See id.* §§ 103-104, 92 Stat. 1783, 1788-90.

295. *See id.* § 102(b), 92 Stat. 1783, 1787. FISA also required that the application list the evidence showing that the foreign power or its agent used or planned to use the site of the surveillance; state the type of surveillance the government planned to use; and list the government's proposed minimization procedures. *See id.* Under FISA, the USFISC judge must make a specific finding that each element of the application is supported by probable cause and that the proposed minimization procedures are proper. *Id.* § 105, 92 Stat. 1783, 1790-93. One of FISA's most important judicial oversight provisions states that the government cannot classify a 'United States person' as "a foreign power or an agent of a foreign power solely upon the basis of activities protected by the [F]irst [A]mendment." *Id.* § 105(a)(3)(A), 92 Stat. 1783, 1790.

296. *See* Helene E. Schwartz, *Oversight of Minimization Compliance under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing Their Job*, 12 RUTGERS L.J. 405, 414-33 (1981). The executive branch of government, through its Attorney General, established minimization procedures as well as internal review procedures and supervision of warrantless surveillance. *Id.* The judiciary could impact the surveillance at three stages: passing on applications, assessing the legality of the surveillance, and imposing civil or criminal liability for violations. *Id.* at 433-72. Finally, reports concerning surveillance pursued under this section had to be submitted to Congress. *Id.* at 472-83.

297. Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, § 106(c), 92 Stat. 1783, 1793.

298. *Id.* § 106(e), 92 Stat. 1783, 1794.

ered an Attorney General's wiretap order presumptively valid, making it difficult for an individual to challenge the legality of the surveillance.[299] In addition, a motion to suppress did not guarantee disclosure of the information to the aggrieved person.[300] The court could disclose the information "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance."[301]

D. The Collision of Title III Evidence Collection and Foreign Intelligence Surveillance

Several provisions of the PATRIOT Act ignore the distinction between the collection of information for domestic criminal investigations and foreign intelligence collection. This destroys the traditional balance between the government and the individual under the Fourth Amendment. Before the PATRIOT Act, in cases assessing motions to suppress or requesting disclosure of FISA-collected information, the courts emphasized the distinction between cases of surveillance under FISA and those under Title III.[302]

In *United States v. Belfield*,[303] the government charged the defendants with "conspiracy to murder, accessory after the fact, grand larceny, unauthorized use of a vehicle, and perjury in connection with [an] assassination."[304] The defendants "requested disclosure of any electronic surveillance" concerning them.[305] The government admitted overhearing each of the defendants during electronic surveillance authorized under FISA.[306]

Pursuant to the statute, the district court judge made an *ex parte* determination of the legality of the surveillance after examining the relevant evidence *in camera*.[307] The defendants challenged the procedures on both statutory and procedural grounds.[308] The defendants asserted that the mandatory disclosure provisions of Title III "must be read into FISA

---

299. *See* Conrad, *supra* note 250, at 979 (approving electronic surveillance of illegal bookmaking suspects (citing United States v. Feldman, 535 F.2d 1175, 1180-81 (9th Cir. 1976)); United States v. Turner, 528 F.2d 143, 150-51 (9th Cir. 1975) (approving interception of wire communications of alleged narcotics conspirators).

300. *See* Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, § 106(f), 92 Stat. 1783, 1794. By filing an affidavit under oath that the disclosure of the information would harm the national security of the United States, the Attorney General may request an *ex parte* determination of the legality of the surveillance based upon an in camera examination of the relevant materials. *Id.*

301. *Id.*

302. *See* United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir. 1982).

303. 692 F.2d 141, 143.

304. *See id.* at 143.

305. *Id.*

306. *Id.*

307. *See id.* at 144.

308. *See id.*

to save it from constitutional infirmity."[309] The District of Columbia Circuit Court of Appeals rejected this argument, stating:

> Appellants . . . completely ignore the nature of the national interests implicated in matters involving a foreign power or its agents. [Title III] covers domestic, criminal surveillance. FISA is concerned with foreign intelligence surveillance. In the former, Congress emphasized the privacy rights of U.S. citizens. In the latter, Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements.[310]

The statutory scheme under FISA "center[ed] on an expanded conception of minimization that differs from that which governs law-enforcement surveillance."[311] Pursuant to FISA, the court merely determines whether the application and order comply with the statutory requirements: "No further judicial procedures are necessary to adequately safeguard appellants' rights."[312] This differs from the standard of checks and balances that characterizes domestic criminal law.

Perhaps because of this, the courts have tended to condemn domestic warrantless electronic surveillance, even if the target posed a "domestic threat[] to the national security."[313] By contrast, when the circumstances involved surveillance of foreign nationals, the lower courts generally upheld the surveillance.[314] When the surveillance had both domestic criminal investigative and foreign intelligence purposes, however, the lower courts upheld the warrantless electronic surveillance of American citizens despite its impact on the rights of the accused.[315]

---

309. *See id.* at 148. The defendants relied on section 2518 of Title III, which provides that "the contents of an intercepted communication may not be used in any proceeding unless the aggrieved person is first furnished with a copy of the application and the court order authorizing the interception." *See id.* at 184 n.31.

310. *Id.* at 148.

311. *See id.* (citing Helene E. Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing Their Job*, 12 RUTGERS L.J. 405, 408 (1981)).

312. *See id.* at 149.

313. *See, e.g., United States Dist. Court*, 407 U.S. at 320, 322, 323-24.

314. *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 914-15 (4th Cir. 1980); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974).

315. *See, e.g.*, United States v. Clay, 430 F.2d 165, 170-71 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971). The government sought to use the results of wiretaps in its case against Muhammad Ali, then known as Cassius Clay, for violating the Selective Service Act. *Clay*, 430 F.2d at 166. While ordering disclosure of four of the five conversations, the court of appeals upheld the district court's conclusion that the fifth wiretapped conversation resulted from "lawful surveillance by the FBI pursuant to the Attorney General's authorization of a wiretap for the purpose of gathering foreign intelligence," and therefore would not be disclosed to Clay. *See id.* at 166, 171; *see also* United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) (affirming the President's power

The information-sharing agreements enjoyed by the various intelligence groups and the FBI partly made possible the abuses of the 1970s. The Church Committee Report documented a CIA-FBI agreement that improved the intelligence coordination between the two agencies. "[T]he policies embodied in that agreement clearly involved the CIA in the performance of internal security functions."[316] In essence, requiring the FBI and the CIA to cooperate in intelligence collection circumvented the National Security Act's prohibition against the CIA's participation in domestic intelligence gathering.[317] The CIA's partnership with the FBI did not make this practice legitimate.[318]

E. Broadened Scope of FISA Surveillance on the Domestic Front Under the PATRIOT Act

Congress enacted FISA to curtail these abuses, but President Reagan reintroduced the CIA-FBI partnership model in Executive Order 12,333.[319] The PATRIOT Act augments this type of partnership on an unprecedented scale. It also magnifies the potential for government violation of the individual's privacy. Section 905 of the PATRIOT Act requires that other agencies share with the Director of the CIA any "foreign intelligence" collected in the course of federal criminal law investigations, unless the Attorney General makes exceptions.[320]

Under section 203, sensitive personal, political, and business information about any individual or company collected in the course of a grand jury, domestic law enforcement wiretap, or any other criminal investigation must now be disclosed to any intelligence, defense, and national security agency if the information involves foreign intelligence.[321]

---

to "authorize warrantless wiretaps" to gather foreign intelligence in circumstances where the government incidentally overheard an American citizen's conversations).

316. Conrad, *supra* note 250, at 971; *see also* S. REP. NO. 94-755, at 97 (1976).

317. *See* Conrad, *supra* note 250, at 973-74 (discussing the CIA's exclusion from domestic operations).

318. *See id.* at 981-82 (discussing Exec. Order No. 12,3333 and other agreements that sought to improve the coordination between the CIA and the FBI).

319. *See id.* President Regan promulgated Executive Order 12,333 in 1981. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981). The order delegated to the Attorney General the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. *Id.*

320. USA PATRIOT Act, Pub. L. No. 107-56, § 905(a)(2), 115 Stat. 272, 389.

321. *See id.* § 203, 115 Stat. 272, 279-81. Foreign intelligence is defined as "information relating to the capabilities, intentions or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities." 50 U.S.C. § 401a(2) (2000). Foreign intelligence information includes "information about a United States person that concerns a foreign power or foreign territory and 'that relates to the national defense or the security of the United States.'" *See* 147 CONG. REC. S10990-02, S10992 (daily ed. Oct. 25, 2001).

Americans have generally felt free to conduct business and personal relationships with foreign governments or nationals and to express personal opinions about governmental policy without recourse. These communications could be entirely legal, but they could also fit the definition of foreign intelligence information. As such, the PATRIOT Act makes these communications eligible for broad dissemination to any government official.[322]

While prior law allowed information sharing between grand juries, the court supervised the disclosure of such information.[323] Section 203 does not provide such oversight of these information-sharing activities and does not limit the purposes for which the information can be disclosed. Section 203 creates a fundamental change in the existing criminal justice system, as Congress did not limit its scope to investigations about terrorism.

The indiscriminant sharing of information ignores the radically different purposes of the domestic criminal law system and that of foreign intelligence gathering.[324] Unlike domestic criminal law investigations, foreign intelligence surveillance may not consider the ultimate truth of the information collected as an objective. A disclosure of innuendo and inference may significantly harm an individual's reputation. A system that lacks checks and balances will likely disclose inaccurate or incomplete information.

In the course of an ordinary criminal investigation, the government may collect information on individuals not involved in any illegal activity. The lack of guidelines for using this information exacerbates the potential for misuse during any information-sharing activities.

> Many individuals are investigated and later cleared. Many cases are investigated and never prosecuted. Many witnesses are interviewed whose testimony never surfaces at trial. Immunity is granted to compel testimony before grand juries about people who are never indicted. Wiretaps and microphone "bugs" and computer communications intercepts pick up extensive information about activities and

---

322. *See* 147 CONG. REC. S10990-02, S10992 (daily ed. Oct. 25, 2001).

323. *Id.* at S11005-06.

324. *See* S. REP. NO. 95-701, at 12-13 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3981.

> The criminal laws are enacted to establish standards for arrest and conviction; and they supply guidance for investigations conducted to collect evidence for prosecution. Foreign counterintelligence investigations have different objectives. They succeed when the United States can insure that an intelligence network is not obtaining vital information. . . . Prosecution is a useful deterrent, but only where the advantages outweigh the sacrifice of other interests. Therefore, procedures appropriate in regular criminal investigations need modification to fit the counterintelligence context.

Id.; *see also* Brown & Cinquegrana, *supra* note 248, at 133.

> opinions and personal lives that have no relevance to the criminal activity they are authorized to detect or monitor. [325]

The standard for the collection of this information requires only that investigators consider it "relevant to an investigation."[326] Despite this, section 203 allows broad disclosure within the law enforcement community of information falling under the heading of foreign intelligence or foreign intelligence information, further detaching it from its original relevance. The government could use information collected under FISA's relevance standard in a domestic criminal law investigation employing a probable cause standard. This would violate the rights of the individual. Without limitations on its retention, this information collection could lead to the return of the abuses of the 1970s with development of secret dossiers on individuals.

Section 218 of the PATRIOT Act amends the definition of the term "foreign intelligence information,"[327] which compounds the concerns over the broad dissemination of information about individuals under section 203. FISA provided a lowered standard for foreign intelligence surveillance, but restricted its use to circumstances where obtaining foreign intelligence data represented the sole or primary purpose of the investigation.[328] Section 218 of the PATRIOT Act amends FISA to apply in situations where foreign intelligence collection represents only a "significant purpose" of the investigation.[329]

The amendment further blurs the lines between acceptable foreign intelligence gathering on a reasonableness standard and the probable cause requirements of domestic criminal investigations. If the government conducts surveillance by wiretap for the purpose of obtaining information relevant to both a domestic criminal investigation and foreign intelligence activities, the government could avoid the probable cause requirements of Title III. The individual would lose vital privacy protection as a result. This "would be a significant alteration to the delicate constitutional balance that is reflected in the current legal regime governing electronic surveillance."[330]

F. Broad Access to Records and Other Items Under FISA

Section 215 of the PATRIOT Act amends FISA by giving the government the authority to require the production of "any tangible things (including books, records, papers, documents, and other items) for an

---

325. 147 CONG. REC. S10990-02, S10992 (daily ed. Oct. 25, 2001).
326. *See id.*
327. USA PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291.
328. *See* EPIC, *supra* note 207.
329. USA PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291.
330. *See* EPIC, *supra* note 207 (discussing a similar provision of a predecessor bill).

investigation to protect against international terrorism or clandestine intelligence activities."[331] Although narrowly circumscribed on its face, section 215 provides that the government conduct such investigations "under guidelines approved by the Attorney General under Executive Order No. 12,333."[332] This has potentially serious consequences for privacy.

Pursuant to Executive Order No. 12,333, "Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General."[333] The fact that the procedures established by the Attorney General are themselves "not subject to review . . . by any public body" raises concerns. [334] The Order allows the Attorney General to authorize "any technique for which a warrant would [ordinarily] be required . . . [upon a unilateral judgment] that the technique is directed against a foreign power or an agent of a foreign power."[335] The lack of a definition for the term "agent of a foreign power" means that the characterization of the target falls exclusively within the discretion of the Attorney General as well.[336]

While the FBI must apply for an order to the special FISA court, the court will grant the order on less than probable cause.[337] The government need only certify that it seeks the records for an authorized investigation conducted pursuant to the Attorney General's procedures, and that the investigation intends to obtain foreign intelligence information, a very broadly defined term.[338] Since the Attorney General has the sole discretion to define the parameters of the investigation, the government obtains access to a broad range of private records in potential violation of the individual's privacy.

Section 905 of the PATRIOT Act further reduces the individual's sphere of privacy by requiring law enforcement agencies to share sensitive "foreign intelligence information" about Americans with intelligence agencies through the Director of the CIA, unless the Attorney General

---

331. USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287.

332. *See id.* President Ronald Reagan issued Executive Order No. 12,333, which greatly expanded the authority of the Central Intelligence Agency to conduct domestic intelligence operations. *See* Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

333. Exec. Order No. 12,333, 46 Fed. Reg. 59,941, § 2.4.

334. *See* Conrad, *supra* note 250, at 977.

335. Exec. Order No. 12,333, 46 Fed. Reg. 59,941, § 2.5.

336. *See* Conrad, *supra* note 250, at 979.

337. *See supra* notes 292-301 and accompanying text for a discussion of FISA.

338. *See* definition of "foreign intelligence information," *supra* note 321.

makes exceptions.[339] As history has shown, such arrangements increase the potential for governmental overreaching.

Despite their descriptive titles, "foreign intelligence" and "foreign intelligence information" could include sensitive information about an individual's lawful business transactions, political relationships, and personal opinions concerning members of a foreign government.[340] The First and Fifth Amendments by virtue of the Fourth Amendment currently protect these activities. However, a legislative enactment that removes them from constitutional protection implies that society no longer recognizes the individual's subjective expectation of privacy in these records as legitimate.

Over the years, various Executive Orders have modified the express bar to domestic authority, but it would seem that any further extension to the CIA's domestic surveillance power would contravene its charter under the National Security Act.[341]

Section 506 of the PATRIOT Act gives concurrent jurisdiction to the Secret Service to investigate certain computer-related offenses under 18 U.S.C. § 1030.[342] This returns the Secret Service to the full authority it had before 1996 to investigate any and all violations of section 1030.[343] Ostensibly, this extension of authority allows the Secret Service to protect critical infrastructures from terrorist attacks.[344] Like many other provisions of the PATRIOT Act, Congress did not limit this change by the terms of the Act, and it becomes a permanent feature of our criminal laws.

---

339. USA PATRIOT Act, Pub. L. No. 107-56, § 905(a)(2), 115 Stat. 272, 389; *see supra* text accompanying note 32; *see also* 147 CONG. REC. S10990-02, S10992 (daily ed. Oct. 25, 2001).

340. *See* definition of "foreign intelligence," *supra* note 321.

341. For instance, President Carter's Executive Order No. 12,036 prohibited surveillance against United States persons abroad. Exec. Order No. 12,036, 43 Fed. Reg. 3674, § 2-202 (Jan. 24, 1978). President Reagan's Executive Order No. 12,333, however, allows such surveillance "even if the CIA has no reason to believe the target is . . . an 'agent of a foreign power.'" *See* Conrad, *supra* note 250, at 978.

342. USA PATRIOT Act, Pub. L. No. 107-56, § 506(a), 115 Stat. 272, 367. In 1995, the Secret Service created the New York Electronic Crimes Task Force ("NYECTF"). *See* 147 CONG. REC. S10990-02, S10998 (daily ed. Oct. 25, 2001). This group includes members from industry law enforcement and academia and "has successfully investigated a range of financial and electronic crimes." *Id.* Section 105 of the PATRIOT Act authorizes the Secret Service to create similar task forces in other parts of the country. *Id.*

343. *See* 147 CONG. REC. S10990-02, S10998 (daily ed. Oct. 25, 2001). The 1996 amendments to section 1030 concentrated the authority of the Secret Service on specific sections of the Computer Fraud and Abuse Act. *Id.* Section 506 of the PATRIOT Act permits the Justice and Treasury Departments to work out the parameters of the new concurrent jurisdiction. *Id.*

344. *Id.*

G. Privacy Protection Under Title III (Wiretap Statute)

> *Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.*[345]

When first confronted with the issue of whether wiretapping violated the Fourth Amendment in *Olmstead v. United States*,[346] the Supreme Court held that wiretapping did not constitute a search.[347] However, even the majority recognized the danger of permitting unrestrained governmental surveillance and suggested a practical limitation to guard against governmental overreaching. The Court noted, "Congress may of course protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials."[348] The Court ultimately overturned the *Olmstead* decision in *Katz v. United States*.[349]

The Federal Communications Act of 1934 ("FCA")[350] did not explicitly adopt the Court's suggestion for the protection of privacy. However, some interpreted certain language in the FCA as statutory authority for the existence of the *Olmstead* exclusionary rule. Section 605 of the FCA provided, "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[351] The Court interpreted section 605 to prevent testimony concerning the contents of wiretapped conversations in court because "to recite the contents of the message in testimony before a court [would be] to divulge the message."[352] The Court later held the exclu-

---

345. *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting).

346. 277 U.S. 438.

347. *Id.* at 466. The Court provided two bases for its decision. First, there had been no entry of the premises that would give rise to a search. *Id.* Second, while the agents "captured" the content of the conversations, they had not acquired any physical objects that would constitute a seizure. *Id.* This trespass model was followed by the Court in a number of decisions, including *Goldman v. United States*, 316 U.S. 129 (1942) (placing a detectaphone against a wall of an adjoining office where the police were lawfully present did not constitute a trespass), and *On Lee v. United States*, 343 U.S. 747 (1952) (incriminating information from bug planted on an acquaintance of target by consent).

348. *Olmstead*, 277 U.S. at 465.

349. 389 U.S. 347, 353.

350. Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934). The FCA was the first federal statute to establish procedural protections against electronic surveillance by the government.

351. *Id.* § 605, 48 Stat. 1064, 1068.

352. *Nardone*, 302 U.S. 379.

sionary rule applicable to derivative evidence,[353] to intrastate communications,[354] and to the actions of state officers.[355]

Section 605 frustrated both law enforcement and privacy advocates. It allowed private citizens and public officials to ignore its prohibitions, but banned the use of electronic surveillance in police investigations for even the most serious of federal offenses.[356] Since the FCA did not preempt state law, state criminal prosecutors could admit wiretaps that did not meet section 605's standards.[357] Finally, section 605 did not bar intelligence surveillance.[358] The government continued to use wiretaps to collect foreign intelligence for national security purposes.[359] The government supported this continued use with the rationale that it could lawfully "intercept" communications, but not "divulge" them.[360] Further, the government contended that it did not divulge information in its internal communications, but only if it released the information to an outside party.[361] Foreign intelligence surveillance rarely resulted in prosecution, leaving little chance that the government would divulge an intercepted communication.

Since no legislature had codified the *Olmstead* exclusionary rule, courts did not have to follow it. The sphere of the individual's privacy received uneven treatment in courts called upon to determine whether to admit or exclude evidence produced from wiretaps.[362] Recognizing the need for substantive restraint against police action, the courts ultimately upheld the validity of the exclusion. In *Lee v. Florida*,[363] the Court stated that the exclusionary rule was "counseled by experience."[364] The Court's research of section 605 violations had "failed to uncover a single reported prosecution of a law enforcement officer for a violation of s[ection] 605 since the statute was enacted."[365] The Court "concluded . . . that nothing short of mandatory exclusion of the illegal evidence [would]

353. *See* Nardone v. United States, 308 U.S. 338, 341 (1939).

354. *See* Weiss v. United States, 308 U.S. 321, 329 (1939).

355. *See* Benanti v. United States, 355 U.S. 96, 100 (1957).

356. WAYNE LAFAVE, CRIMINAL PROCEDURE 261 (3d ed. 2000).

357. *See* JAMES G. CARR, THE LAW OF ELECTRONIC SURVEILLANCE § 2.4(a) (2d ed. 1989).

358. *See* Herbert Brownell, Jr., *The Public Security and Wiretapping*, 39 CORNELL L.Q. 195, 197-99 (1954); John F. Decker & Joel Handler, *Electronic Surveillance: Standards, Restrictions and Remedies*, 12 CAL W. L. REV. 60, 63-64 (1975).

359. *See* Brownell, *supra* note 358, at 199.

360. *See id.* at 197.

361. *See* Decker & Handler, *supra* note 358, at 64.

362. *See* Lee v. Florida, 392 U.S. 378, 386-87 (1968) (evidence excluded); Mapp v. Ohio, 367 U.S. 643, 660 (1961) (evidence excluded); *Benanti*, 355 U. S. at 105-06 (evidence excluded); Schwartz v. Texas, 344 U.S. 199, 203 (1952) (evidence admitted), *overruled by Lee*, 392 U.S. at 386-87; Wolf v. Colorado, 338 U.S. 25, 33 (1949) (evidence admitted), *overruled by Mapp*, 367 U.S. at 660.

363. 392 U.S. 378.

364. *Lee*, 392 U.S. at 386.

365. *Id.*

compel respect for the federal law 'in the only effectively available way -- by removing the incentive to disregard it.'"[366]

In addition to these failings, it became clear that section 605 could not keep pace with the advances in surveillance technology.[367] In order to balance law enforcement's need to use the latest technology with the individual's right to some degree of privacy, Congress enacted Title III.[368] Congress intended Title III to protect privacy by defining a uniform procedure for the "interception of wire and oral communications."[369] Only a "court of competent jurisdiction" could authorize such interception.[370] In this manner, the statute safeguarded the privacy of innocent persons who had not consented to the interception of their wire or oral communications.[371] As additional protection, Congress required that the interception remain under the control and supervision of the authorizing court.[372]

Section 2518 provided a template for obtaining court-approved interception and listed the contents of a valid application for court ordered surveillance.[373] It also restricted the scope and duration of the surveillance.[374] Title III provided several layers of privacy protection. A court would issue a warrant for the interception if the government met the provision's detailed probable cause requirements.[375] The standard under Title III required probable cause to believe that "an individual [was] committing, ha[d] committed, or [was] about to commit" one of the enumerated offenses, and that "particular communications concerning that offense [would] be obtained through such interception."[376] It required that the order state with specificity the target's identity, the location of the interception, the identity of the agency authorized to intercept,

---

366. *Id.* at 386-87 (quoting Elkins v. United States, 364 U.S. 206, 217 (1960)).

367. *See* LAFAVE, *supra* note 356, at 260.

368. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2000)). Title III was part of the Omnibus Crime Control and Safe Streets Act of 1968. Congress noted that "there [had] been extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversations." *Id.* § 801, 82 Stat. 197, 374-75.

369. *Id.*

370. *Id.*

371. *See id.*

372. *Id.*

373. *Id.* § 802, 82 Stat. 197, 261-62.

374. *Id.* § 802, 82 Stat. 197, 263.

375. *Id.* § 802, 82 Stat. 197, 262. Under Title III, a judge could order a wiretap if he determined, among other things, that probable cause existed to believe "that an individual is committing, has committed, or is about to commit" one of the enumerated offenses and "the facilities from which, or the place where, the . . . communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person." *Id.*

376. *Id.*

and the identity of the person authorizing the interception.[377] It also required a statement of whether the interception must cease immediately upon obtaining the communication described in the application.[378] Strict duration requirements also attached.[379]

This heightened probable cause requirement reflected the heightened privacy intrusion presented by wiretaps.[380] Wiretaps differ from physical search warrants in that the orders allow continuing surveillance for up to 30 days with possible extensions.[381] The government could overhear all conversations transpiring during that period without regard to relevancy.[382] "Only the most precise and rigorous standard of probable cause should justify an intrusion of this sort."[383] The failure to obtain an order would result in the invalidation of even narrowly tailored surveillance.[384]

However, Title III carved out an exemption for wiretapping performed in the pursuit of foreign intelligence gathering.[385] It did not limit the constitutional power of the President to "obtain[ing] foreign intelligence information deemed essential to the security of the United States, or to protect[ing] national security information against foreign intelligence activities."[386] Restrictions on the executive's use at trial of information obtained pursuant to this section provided additional privacy protection. The government could use the information only if the "interception was reasonable," and it could not otherwise disclose the information except as necessary for the executive to implement his power to protect the nation.[387]

Over the years, Congress added three additional sections, 2511, 2515, and 2520, to provide remedies for violations of Title III. These sections provided for criminal sanctions,[388] injunctive relief,[389] civil remedies,[390] and the right to exclude the contents of the illegally obtained

377. *Id.* § 802, 82 Stat. 197, 263.

378. *Id.*

379. *Id.*

380. *See Berger*, 388 U.S. at 58-63.

381. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 263.

382. *But see* discussion on Carnivore, *supra* note 240.

383. *See Berger*, 388 U.S. at 69 (Stewart, J., concurring).

384. *Katz*, 389 U.S. at 354 ("surveillance was so narrowly circumscribed that a duly authorized magistrate, . . . clearly apprised of the precise intrusion it would entail, could constitutionally have authorized, with appropriate safeguards, the very limited search and seizure that the Government asserts in fact took place").

385. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 257. This exemption has particular significance to some of the provisions of the PATRIOT Act.

386. *Id.*

387. *Id.*

388. 18 U.S.C. § 2511(4) (2000).

389. *Id.* § 2511(5).

390. *Id.* § 2520.

communications from evidence.[391] According to the U.S. Attorney statistics, these remedies have not hindered the government's surveillance ability.[392]

H. Expansion of Government Ability to Intercept Communication Under FISA

Title III provided several layers of privacy protection to the individual because of the intrusive nature of electronic surveillance. Before the PATRIOT Act, FISA did not significantly deter government surveillance if the information sought fell under the heading of foreign intelligence. The PATRIOT Act's amendments to FISA weaken even those restrictions.

FISA required the government to certify that the targeted communication came from an individual engaging in international terrorism or an agent of a foreign power.[393] Section 214 of the PATRIOT Act eliminates this requirement.[394] This means that the government could justify surveillance with a pen register/trap and trace device by alleging that it intended to use the device in "any investigation to obtain foreign intelligence information,"[395] a much more lax standard. This circumvents FISA's limited protection against governmental intrusions and undercuts the reasons for a lowered standard for governmental surveillance.[396] This amendment allows the government to perform searches for customary purposes, but without the protection of the probable cause requirement in regular criminal investigations.

I. Multi Point (Roving Wiretap) Authority

Section 206 of the PATRIOT Act amends FISA to include "roving" wiretap authority. Roving wiretaps for domestic criminal law investigations require third parties "'specified in court-ordered surveillance' to provide assistance . . . to accomplish the surveillance" on a communica-

---

391. *Id.* § 2515. This section codifies the *Olmstead* exclusionary rule. *See Olmstead*, 277 U.S. at 468, *overruled in part by Berger*, 388 U.S. 41 and *Katz*, 389 U.S. 347.

392. As stated by Justice Holmes in his dissent in *Olmstead*, "[I]t [is] a less evil that some criminals should escape than that the government should play an ignoble part." *See Olmstead*, 277 U.S. at 470 (Holmes, J., dissenting).

393. 50 U.S.C. § 1842(c)(3) (2000).

394. USA PATRIOT Act, Pub. L. No. 107-56, § 214, 115 Stat. 272, 286.

395. *Id.*

396. Electronic Privacy Info. Ctr., *Foreign Intelligence Surveillance Act (FISA)*, *at* http://www.epic.org/privacy/terrorism/fisa/ (last visited Nov. 10, 2002) [hereinafter EPIC FISA].

> That laxity is premised on the assumption Congress and the courts should not unduly restrain the Executive branch, in pursuit of its national security responsibilities to monitor the activities of foreign powers and their agents. The removal of the "foreign power" predicate for pen register/trap and trace surveillance upsets that delicate balance.

Id.

tion as it moves through a succession of carriers and devices, i.e., roves.[397] Pursuant to section 206 of the PATRIOT Act, the FISA roving wiretap order need not identify the third party if the "[c]ourt finds that the actions of the target . . . may have the effect of thwarting the identification of a specified person."[398] The proposed change would extend the obligation to assist the government "to unnamed and unspecified third parties."[399] Upon the discovery of a new carrier, the government would present it with a generic wiretap order and "effect FISA coverage as soon as technically feasible."[400] The PATRIOT Act has very little of the protections afforded under Title III.

The PATRIOT Act particularly threatens the privacy of individuals who access the Internet through public facilities, such as libraries and university computer labs.[401] "Upon the suspicion that an intelligence target might use such a facility, the FBI [could] . . . monitor all communications transmitted at the facility."[402] There exists a high probability that the government could intercept "the private communications of law-abiding . . . citizens" since "the recipient of the assistance order . . . would be prohibited from disclosing the fact that monitoring is occurring."[403]

CONCLUSION

Surveillance technology will invariably advance and terrorists will invariably use those advancements. No one would suggest that the government should not use the most current technology to prevent tragedy. However, protection does not mean that we should abandon traditional notions of privacy. As a society, we may choose to cede more of our civil liberties so as to prevent another 9/11, but we should not make this decision lightly or without fully understanding what we put at risk.

Interpreting the Fourth Amendment to cover both physical and non-physical governmental intrusions, the courts balanced the government's need to search purportedly private areas with the individual's need to prevent government intrusion.[404] The complex system of safeguards de-

397. *See* EPIC, *supra* note 207.

398. USA PATRIOT Act, Pub. L. No. 107-56, § 206, 115 Stat. 272, 282.

399. EPIC, *supra* note 207.

400. *Id.*

401. *See* EPIC FISA, *supra* note 396.

402. *See id.*

403. *See id.*

404. *See generally* Kyllo v. United States, 533 U.S. 27 (2001) (holding that sense-enhancing surveillance technology intrudes upon minimum expectation of privacy protected under the Fourth Amendment); United States v. Karo, 468 U.S. 705 (1984) (placing unmonitored surveillance device to track use of drug extracting equipment did not violate Fourth Amendment because it did not intrude on reasonable expectation of privacy); Katz v. United States, 389 U.S. 347 (1967) (holding that defendant justifiably relied on privacy of public telephone booth and that it would be free from unwarranted electronic surveillance by government); Carroll v. United States, 267 U.S. 132 (1925)

veloped to support the Fourth Amendment provides evidence of the nation's resolve to maintain that balance. Judicial oversight balanced the needs of the government with the privacy interests of citizens by enforcing the requirement for warrants and by assessing the reasonableness of searches performed. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 established the procedural guidelines for the use of wiretapping and electronic eavesdropping by law enforcement agencies.[405] Exclusionary rules created an incentive for law enforcement officials to obey these constraints by precluding the suppression of evidence properly obtained through the use of warrants.[406] The Electronic Communications Privacy Act gave procedures for obtaining access to stored electronic communications (e-mail).[407]

Removal of the checks and balances on governmental action by the PATRIOT Act could diminish the already waning protection afforded by the Fourth Amendment. By increasing the scope of information subject to government access and reducing the independent judicial review of the government's actions, the PATRIOT Act lowered the threshold for legitimate governmental intrusion into the individual's privacy under the Fourth Amendment.

> [I]f the government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation or [sic] privacy regarding their homes, papers, and effects. . . . In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth amendment protection was.[408]

Without Congressional oversight, the PATRIOT Act could render the Fourth Amendment impotent as a guardian of civil liberty in domestic criminal law investigations. In the words of Ben Franklin, one of the

---

(holding that the government must show probable cause to seize vehicles for transport of liquor in the absence of a warrant to protect motorist's freedom from seizure under Fourth Amendment).

405. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2000)). The Electronic Communications Privacy Act of 1986 amended Title III by including such electronic communications as digitally transmitted conversations, electronic mail, cellular telephones and pen registers. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

406. FED. R. CRIM. P. 41.

407. 18 U.S.C. § 2703 (Supp. IV 1987).

408. Smith v. Maryland, 442 U.S. 735, 741 n.5 (1979).

founding fathers of this nation, "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."[409]

409. Benjamin Franklin, *Historical Review of Pennsylvania*, *in* JOHN BARTLETT, FAMILIAR QUOTATIONS 310 (Justin Kaplan ed., 16th ed. 1992).