

2002

Hijacking Civil Liberties: The USA PATRIOT Act of 2001

Jennifer C. Evans

Follow this and additional works at: <http://lawcommons.luc.edu/lucj>



Part of the [Law Commons](#)

Recommended Citation

Jennifer C. Evans, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001*, 33 Loy. U. Chi. L. J. 933 (2002).
Available at: <http://lawcommons.luc.edu/lucj/vol33/iss4/13>

This Comment is brought to you for free and open access by LAW eCommons. It has been accepted for inclusion in Loyola University Chicago Law Journal by an authorized administrator of LAW eCommons. For more information, please contact law-library@luc.edu.

Comment

Hijacking Civil Liberties: The USA PATRIOT Act of 2001

Jennifer C. Evans*

I. INTRODUCTION

Almost a decade ago on February 26, 1993, six people were killed and over one thousand others were injured when terrorists bombed the World Trade Center in New York City.¹ On April 19, 1995, one hundred sixty-eight people, including nineteen children, were killed when a car bomb exploded in front of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma.² On August 7, 1998, the bombing of United States embassies in Nairobi, Kenya and Dar es Salaam, Tanzania, killed 225 people.³ Two years later, on October 12,

* J.D. expected May 2003. I would like to thank the members of the Loyola University Chicago Law Journal for their comments and suggestions. To my parents and sister, your support and encouragement mean everything.

1. Diplomatic Security Service, U.S. Department of State, *World Trade Center Bombing*, at <http://www.dssrewards.net/english/wldtrade.html> (last modified Jan. 9, 2002). On April 3, 1998, Eyad Ismoil was sentenced to 240 years imprisonment with no hope of parole after being convicted in November 1998 on conspiracy charges for his role in the 1993 World Trade Center bombing. CNN Interactive, *Last World Trade Center bombing conspirator sentenced*, at <http://www.cnn.com/US/9804/03/wtc.bombing/> (last modified Apr. 15, 2002). Five other conspirators were given the same 240-year sentence, including Ramzi Yousef, the alleged mastermind of the attack. *Id.*

2. CNN Interactive, *Oklahoma City Tragedy: The Bombing*, at <http://www.cnn.com/US/OKC/bombing.html> (last modified Feb. 21, 2002). Timothy McVeigh was found guilty of the Oklahoma City federal building bombing. CNN Interactive, *The McVeigh Trial: After 28 days of 'overwhelming evidence,' the jury speaks: Guilty*, available at <http://www.cnn.com/US/9706/171McVeigh.overview/> (last visited Mar. 25, 2002). McVeigh was sentenced to death by lethal injection. *Id.* Terry Nichols was also convicted of the Oklahoma City bombing, sentenced to life imprisonment, and ordered to pay the government \$14 million for the damages to the federal building. CNN Interactive, *Nichols gets life for Oklahoma Bombing*, available at <http://www.cnn.com/US/9703/okc.trial/nichols.sentence> (last modified Apr. 15, 2002).

3. Jim Fisher-Thompson, *U.S. Gives Kenya, Tanzania \$46 Million in Bombing Aftermath*, United States Information Agency, at <http://usinfo.state.gov/topical/pol/terror/98110201.htm> (last modified Nov. 8, 2000). More than 4,000 Kenyans were injured in the explosions. *Id.* Twelve Americans were killed in the Kenyan bombing. *Id.*

2000, a suicide bomber rammed into the side of the Navy destroyer USS Cole, killing seventeen and injuring thirty-eight sailors.⁴ Finally, on September 11, 2001, terrorists hijacked American Airlines Flights 11 and 77 and United Airlines Flights 175 and 93, creating a new weapon of mass destruction by colliding a plane into each tower of the World Trade Center in New York City, another into the Pentagon in Washington, D.C., and finally crashing one into a field in western Pennsylvania.⁵ Approximately 3,225 people were killed on the planes and on the ground.⁶

These tragedies are only a sample of terrorist attacks affecting United States' interests within the past ten years⁷ and represent those with the greatest effect on Americans.⁸ As a result of such attacks, the United States Congress introduced and enacted responsive and reactionary legislation to enable federal law enforcement agencies to investigate terrorist organizations, large and small, domestic and foreign.⁹ This legislation, the USA PATRIOT Act, provides for increased surveillance and the ability to collect intelligence regarding these organizations in order to combat terrorism and protect Americans.¹⁰ While combating terrorism is a priority, much of this legislation chips away at the constitutionally protected rights of citizens and residents of the United States, including the Fourth Amendment's protection from unreasonable searches and seizures.¹¹

4. See Howard Schneider & Roberto Suro, *Death Toll Put at 17 In USS Cole Blast; Some Doubt Yemenis Will Aid in Probe*, WASH. POST, Oct. 14, 2000, at A01, available at 2000 WL 25422178.

5. Charles M. Madigan, 'Our nation saw evil'; *Hijacked jets destroy World Trade Center, hit Pentagon, Thousands feared dead in nation's worst terrorist attack*, CHI. TRIB., Sept. 12, 2001, § 1, at 1, available at 2001 WL 4113876. Officials speculated that Flight 93 was heading for a fourth target in the nation's capital, but due to the heroics of the passengers and its crew, this mission was foiled. *U.S. Strikes Afghanistan*, WASH. POST, Oct. 8, 2001, at C14, available at 2001 WL 28363099.

6. See Margaret Talbot, *The Lives They Lived, 3,225 (At Last Count) Died September 11*, 2001, N.Y. TIMES, Dec. 30, 2001, §6, at 16. Initially, it was estimated that over 6,000 people died in the attacks. *Id.*; see Madigan, *supra* note 5.

7. See *infra* note 176 and accompanying text (discussing terrorist incidents on American soil from 1970–1999).

8. See, e.g., United and Strengthening America—Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

9. *Id.* at 276-78.

10. *Id.* at 278-96.

11. The Fourth Amendment states:

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

Part II of this Comment begins with an overview of the Fourth Amendment, including a discussion of warrantless searches for purposes of national security.¹² Part II summarizes the history of anti-terrorism legislation, focusing primarily on Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (OCCSSA), the Foreign Intelligence Surveillance Act of 1978 (FISA), and the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA).¹³ Part II will also relate a history of the terrorist events of September 11, 2001.¹⁴ Part III discusses the development of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) enacted in October 2001, focusing on increased governmental surveillance powers.¹⁵ Part IV analyzes this legislation and argues that it potentially violates guaranteed Fourth Amendment protections.¹⁶ Finally, Part V demonstrates that Congress and the courts must take an active role in ensuring that this new national security legislation is applied to true cases of terrorism and that the protections of the Fourth Amendment remain intact.¹⁷

II. BACKGROUND

By adopting the Fourth Amendment, the Framers of the Constitution guaranteed individuals within the United States the right to be free from unreasonable government intrusion.¹⁸ Since the American Revolution, the power to engage in foreign intelligence gathering has been vested with the executive branch of the federal government.¹⁹ Fourth Amendment protections, however, have only been applied to domestic

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. Likewise, the First Amendment's protections from guilt by association and other protections for immigrants and foreign visitors are at risk of erosion, as much of this new legislation allows for the extended detainment of foreign nationals. *See* ACLU, *USA PATRIOT Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances, an ACLU Legislative Analysis* (Nov. 1, 2001), at <http://www.aclu.org/congress/L110101a.html> [hereinafter *ACLU Legislative Analysis*].

12. *See infra* Part II.A–B (providing an overview of Fourth Amendment law).

13. *See infra* Part II.C–D (discussing the development of national security legislation).

14. *See infra* Part II.E (describing the events of September 11, 2001).

15. *See infra* Part III (narrating the development of the USA PATRIOT Act).

16. *See infra* Part IV (analyzing the USA PATRIOT Act).

17. *See infra* Part V (calling for strict Congressional and judicial oversight).

18. *See infra* Part II.A (providing an overview of basic Fourth Amendment requirements).

19. *See infra* Part II.C (discussing early American intelligence activity, the roles of the President and Congress, and the Executive branch's broad use of these powers).

and foreign electronic intelligence gathering since the mid-twentieth century.²⁰

In the 1960s, Congress became aware of abuses of power occurring throughout the intelligence community and its agencies and enacted legislation to provide oversight of these agencies.²¹ The underlying purposes of this legislation were to protect the right of individuals to be free from oppressive government invasion, the right to notice of unreasonable searches and seizures by government actors, and the right to reasonable privacy.²² The most recent national security legislation, the USA PATRIOT Act of 2001, was enacted as a response to the terrorist acts of September 11, 2001, and may potentially violate the civil liberties and protections granted to individuals by the Fourth Amendment.²³

A. *The Fourth Amendment*

The Fourth Amendment to the United States Constitution²⁴ guarantees that individuals in America will be free from unreasonable searches²⁵ and seizures²⁶ by government agents.²⁷ The Framers of the

20. See *infra* Part II.B (discussing the application of the Fourth Amendment to electronic surveillance and national security investigations).

21. See *infra* Part II.C–D (discussing the development of modern intelligence and anti-terrorism legislation).

22. See *infra* Part II.A (discussing protections established by interpretation of the Fourth Amendment).

23. See *infra* Part II.E (discussing the events of September 11, 2001).

24. U.S. CONST. amend. IV.

25. A search is “a governmental invasion of a person’s privacy.” See *Oliver v. United States*, 466 U.S. 170, 177–78 (1984); see also *Katz v. United States*, 389 U.S. 347, 350 (1967) (The Fourth 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.”). See generally Seanna M. Beck, *Thirtieth Annual Review of Criminal Procedure, I. Investigation and Police Practices, Overview of the Fourth Amendment*, 89 GEO. L.J. 1055, 1056–61 (2001) (providing an overview of the search and seizure requirement of the Fourth Amendment).

26. A person is seized “only if, in view of all of the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave.” *United States v. Mendenhall*, 446 U.S. 544, 554 (1980). Property is seized when governmental intrusion meaningfully interferes with an individual’s possessory interest in that property. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984); see Beck, *supra* note 25, at 1061 (providing an overview of what constitutes a property “seizure” for Fourth Amendment purposes); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 356 (1974) (noting that “‘searches’ and ‘seizures’ are not regulated by the Fourth Amendment except insofar as they bear the requisite relationship to ‘persons, houses, papers, and effects’”).

27. See *Walter v. United States*, 447 U.S. 649, 656 (1980) (holding a government search unreasonable); *Wolf v. Colorado*, 338 U.S. 25, 27–28 (1949) (holding that the Fourth Amendment is applicable to state officials through the Due Process Clause of the Fourteenth Amendment);

Constitution intended the Fourth Amendment to protect individuals from unreasonable governmental intrusion into their private lives.²⁸ Generally, the United States Supreme Court has interpreted the Fourth Amendment to require a warrant supported by probable cause²⁹ for each search and seizure.³⁰ While the Fourth Amendment's purpose is to protect individual privacy rights and prevent unwarranted government intrusions, it is not intended as a general restraint on all police practices but only those that are unreasonable.³¹

Weeks v. United States, 232 U.S. 383, 398 (1914) (stating that the Fourth Amendment limits actions of the federal government, not the individual misconduct of federal officials).

28. Gerald K. Freund, *Look Up in the Sky, It's a Bird, It's a Plane . . . It's Reasonableness*, 20 SW. U. L. REV. 195, 198 (1991). Specifically, Congress included the Fourth Amendment in the Bill of Rights "to protect against indiscriminate and arbitrary general authority which had been asserted by the British against the American Colonies." *Id.* The Fourth Amendment became a constitutional protection from the British general warrant, a search tool giving British authorities unlimited ability to search any person or place at any time, without warning or notice. William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 2-3 (2000).

29. "Probable cause is the level of suspicion required to justify certain governmental intrusions upon interests protected by the Fourth Amendment." Beck, *supra* note 25, at 1062; *see* Ornelas v. United States, 517 U.S. 690, 696 (1996) (stating that probable cause to search exists "where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found"); *Illinois v. Gates*, 462 U.S. 213, 241 (1983) (noting that probable cause deals with "probabilities" which are not technical, but "the factual and practical considerations of everyday life on which reasonable and prudent men . . . act"). Probable cause for an arrest warrant exists when, at the moment of arrest, a prudent person with reasonably trustworthy information would believe that an offense has been or is being committed by the person to be arrested. *Beck v. Ohio*, 379 U.S. 89, 91 (1964).

30. *See* U.S. CONST. amend. IV; FED. R. CRIM. P. 41(c)(1) (2000). A warrant shall be issued when the federal magistrate or state judge "is satisfied that grounds for the application exist or that there is probable cause to believe that they exist." FED. R. CRIM. P. 41(c)(1) (2000); *see* U.S. CONST. amend. IV. The Fourth Amendment does not guarantee an individual a constitutional right to privacy. *See* Freund, *supra* note 28, at 200 (discussing the limits of the Fourth Amendment right to privacy). Instead, "[t]he focus is on whether there was a reasonable expectation of freedom from governmental intrusion." *Id.* Furthermore, Congress designed the Fourth Amendment to protect citizens from governmental intrusion in criminal investigations; however, its application to national security intelligence investigations has proven more difficult to understand. Banks & Bowman, *supra* note 28, at 3-4.

31. *See* *United States v. Mendenhall*, 446 U.S. 544, 553-54 (1980) ("The purpose of the Fourth Amendment is not to eliminate all contact between the police and the citizenry, but 'to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals.'" (citations omitted)); Freund, *supra* note 28, at 198 (discussing the Fourth Amendment's general purpose). "Central to an understanding of the Fourth Amendment . . . is a perception of what police activities, under what circumstances and infringing upon what areas and interests, constitute either a search or a seizure within the meaning of that amendment." 1 W. LAFAYE, *SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT*, § 2.1, at 375 (3d ed. 1996).

Although the Supreme Court generally prefers that a warrant based on probable cause be issued,³² it has carved out several exceptions to the Fourth Amendment's probable cause and warrant requirements.³³ These exceptions, which are very case and fact specific,³⁴ usually are applicable when obtaining a warrant is impracticable.³⁵ The reasonableness of a warrantless search or seizure is generally determined by balancing the individual's Fourth Amendment interests against the legitimate government interests.³⁶

Foreign intelligence gathering is necessary because it allows the executive branch to better protect national security.³⁷ For this reason, when conducting warrantless searches, the executive branch has often relied on the assertion that foreign intelligence searches pose a legitimate exception to Fourth Amendment requirements.³⁸ Even though there are numerous enumerated exceptions to the warrant requirement,³⁹ the Supreme Court has yet to create an exception for warrantless foreign intelligence searches.⁴⁰

32. See *Katz v. United States*, 389 U.S. 347, 357 (1967) (recognizing that the Fourth Amendment imposes a presumptive warrant requirement for searches and seizures, as warrantless searches are usually per se unconstitutional).

33. See Theodore P. Metzler et al., *Thirtieth Annual Review of Criminal Procedure, I. Investigation and Police Practices, Warrantless Searches and Seizures*, 89 GEO. L.J. 1084, 1084-1162 (2001). Metzler discusses the exceptions to the Fourth Amendment warrant requirement, including:

investigatory detentions, warrantless arrests, searches incident to a valid arrest, seizure of items in plain view, exigent circumstances, consent searches, vehicle searches, container searches, inventory searches, border searches, searches at sea, administrative searches, and searches in which the special needs of law enforcement make the probable cause and warrant requirements impracticable.

Id. at 1084; see also 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, 107-08 (1985) (providing an overview of the exceptions to the Fourth Amendment warrant requirement).

34. Metzler et al., *supra* note 33.

35. See Brown & Cinquegrana, *supra* note 33, at 108; see also Metzler, *supra* note 33 (providing examples of when a search warrant may be justified). There may be exceptional circumstances when not obtaining a search warrant may be justified; however, generally a warrant is required. *Johnson v. United States*, 333 U.S. 10, 14-15 (1948).

36. *Delaware v. Prouse*, 440 U.S. 648, 654 (1979).

37. Brown & Cinquegrana, *supra* note 33, at 104-05; see *infra* Part II.C-D (discussing this executive power to conduct foreign intelligence surveillance).

38. See Brown & Cinquegrana, *supra* note 33, at 137; Banks & Bowman, *supra* note 28, at 70-74.

39. See *supra* note 33 (setting forth established warrant exceptions).

40. See *infra* Part II.B (discussing Supreme Court and lower court cases regarding a warrant exception for foreign intelligence cases).

1. The Warrant Requirement and Probable Cause

Probable cause is the level of suspicion required to justify certain governmental intrusions upon protected Fourth Amendment interests.⁴¹ When determining whether probable cause exists, the Supreme Court follows a two-step analysis.⁴² First, a court must consider all of the events leading up to the stop or search.⁴³ Second, the court must decide whether those events, considered from the viewpoint of an “objectively reasonable police officer,” amount to probable cause to permit a search or seizure.⁴⁴ On appeal, findings of historical fact must be reviewed only for clear error, and inferences drawn from those facts must be given due weight.⁴⁵ The ultimate determination regarding probable cause on appeal, however, should be based on a *de novo* review.⁴⁶

Unless the search or seizure falls under a warrant exception, the court requires that a warrant be issued for any governmental search or seizure.⁴⁷ Federal Rule of Criminal Procedure 41 requires that a

41. See *Ornelas v. United States*, 517 U.S. 690, 695 (1996). In *Ornelas v. United States*, petitioners pleaded guilty to possession of cocaine with intent to distribute, but reserved their right to appeal the district court’s denial of their motion to suppress evidence of cocaine found in their car. *Id.* at 691. The district court found there was reasonable suspicion for police officers to stop and question petitioners, and probable cause to remove an interior panel of their car, where police officers found two kilograms of cocaine. *Id.* The Court of Appeals found no clear error in the district court’s ruling, and the Supreme Court reversed and remanded this judgment to the district court. *Id.* at 695, 700; see also *Illinois v. Gates*, 462 U.S. 213, 241 (1983); *Beck v. Ohio*, 379 U.S. 89, 91 (1964); *Brinegar v. United States*, 338 U.S. 160, 176 (1949) (stating that the rule of probable cause requires balancing the privacy expectations of citizens from unreasonable interferences by government with the needs of law enforcement in order to protect the community); *supra* note 29 and accompanying text (discussing *Gates* and *Beck*).

42. *Ornelas*, 517 U.S. at 696.

43. *Id.* The majority stated that, “[this] part of the analysis involves only a determination of historical facts . . .” *Id.*

44. *Id.* This second part of the analysis “is a mixed question of law and fact.” *Id.*

45. *Id.* at 699.

46. *Id.* “The background facts provide a context for the historical facts, and when seen together yield inferences that deserve deference . . . [Similarly,] a police officer may draw inferences based on his own experience in deciding whether probable cause exists.” *Id.* at 699-700. *De novo* review is defined as “[a]n appeal in which the appellate court uses the trial court’s record but reviews the evidence and law without deference to the trial court’s rulings.” BLACK’S LAW DICTIONARY 74 (7th ed. abridged 1996).

47. There are two different types of warrants—arrest warrants and search warrants—each requiring a different evidentiary showing. See Chad R. Bowman, *The Warrant Requirement*, 89 GEO. L.J. 1068 (2001) (describing the difference between arrest warrants and search warrants). To obtain an arrest warrant, law enforcement must have probable cause to believe that a crime has been or will be committed. *Steagald v. United States*, 451 U.S. 204, 213 (1981) (finding law enforcement officer could not legally search for subject of arrest warrant in the home of a third party without first obtaining search warrant, unless exigent circumstances existed or third party consented); *Dunaway v. New York*, 442 U.S. 200 (1979); *Henry v. United States*, 361 U.S. 98

warrant should not be issued without a specific description of the property to be seized or the person or place to be searched.⁴⁸ Generally, warrants must describe, "with particularity," the place to be searched or the persons or things to be seized.⁴⁹

Probable cause is required whether or not the police obtain a warrant for a search or seizure.⁵⁰ When no warrant is obtained prior to a search or seizure, a court must determine whether or not the officer's actions were reasonable such that a magistrate judge would have issued a warrant based on probable cause at the time of the search if one had been sought.⁵¹ An exception⁵² is usually established if it is recognized by the court, the government's interests are legitimate, and the individual's privacy expectations are minimal.⁵³ In this situation, if law

(1959); *see also* Beck, *supra* note 25, at 1062. A search warrant may be granted upon a showing of probable cause that the requesting officer believes the legitimate object of a search is located in a particular place. *Steagald*, 451 U.S. at 213; *Hayden*, 387 U.S. at 307. *But see* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994) (discussing Fourth Amendment requirements for search and seizure and arguing that the Fourth Amendment only requires adherence to a reasonableness standard and does not require a warrant or probable cause).

48. FED. R. CRIM. P. 41(c)(1) (2000). "[The] magistrate judge or state judge shall issue a warrant identifying the property or person to be seized and naming or describing the person or place to be searched." *Id.*; *see* *Terry v. Ohio*, 392 U.S. 1, 20 (1968) (requiring police to obtain a search warrant whenever practicable); *Katz v. United States*, 389 U.S. 347, 357 (1967) (stating that warrantless searches are "per se unreasonable . . . subject only to a few specifically established and well-delineated exceptions").

49. *See* FED. R. CRIM. P. 41(c)(1) (stating that an arrest warrant "shall contain the name of the defendant" and a magistrate "shall issue a warrant identifying the property or person to be seized and naming or describing the person or place to be searched"); *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (stating that the particularity requirement "prevents the seizure of one thing under a warrant describing another").

50. *See* *Johnson v. United States*, 333 U.S. 10, 13-14 (1949); *Carroll v. United States*, 267 U.S. 132, 155-56 (1925).

51. *See* *Terry*, 392 U.S. at 20 (concluding that in cases involving police conduct subject to the warrant clause of the Fourth Amendment, when no warrant is obtained, a determination of "whether 'probable cause' existed to justify the search and seizure which took place" is required).

52. *See* *supra* note 33 and accompanying text (setting forth established warrant exceptions).

53. *See* *United States v. Place*, 462 U.S. 696, 706-07 (1983) (finding personal property, such as luggage, may be briefly detained upon reasonable belief that it contains contraband or criminal evidence); *Terry*, 392 U.S. at 30 (holding that a police officer may stop an individual, briefly question him, and perform a limited pat-down frisk for weapons without a warrant if there is reasonable suspicion of criminal activity); *Warden, Maryland Penitentiary v. Hayden*, 387 U.S. 294, 298-99 (1967) (finding a warrantless search constitutional as delay would endanger the lives of citizens); *see also* *Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 660-61 (1995) (finding special needs of the government may permit warrantless searches in specific circumstances); *Schneekloth v. Bustamonte*, 412 U.S. 218, 219 (1973) (finding warrantless search is valid if an individual voluntarily gives his consent).

enforcement's actions were reasonable, the search or seizure is constitutional.⁵⁴

2. The Evolution of a New Test for the Fourth Amendment

The Supreme Court's original interpretation of the Fourth Amendment's protection from unreasonable searches and seizures focused on privacy as a property concept.⁵⁵ Relying on this concept, the Court in *Olmstead v. United States*⁵⁶ upheld the unwarranted use of wiretaps to intercept the conversations of the defendant and others in a criminal investigation and refused to extend the Fourth Amendment language, "persons, houses, papers, and effects,"⁵⁷ to include telephone wires.⁵⁸

The defendants in *Olmstead* were tried and convicted of conspiring to violate the National Prohibition Act,⁵⁹ largely based on the interception of telephone messages by four federal prohibition officers.⁶⁰ The

54. *Terry*, 392 U.S. at 20-21.

55. Banks & Bowman, *supra* note 28, at 42. The Supreme Court first seriously considered the nature of the Fourth Amendment in *Boyd v. United States*, holding that a person's private papers could not be seized and used as evidence against him in a criminal proceeding. *Boyd v. United States*, 116 U.S. 616, 638 (1886). The defendant was charged with fraud and was ordered to produce certain invoices regarding goods it imported into the United States. *Id.* at 617-18. The Court stated, "[i]t 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" which is prohibited by the Fourth Amendment. *Id.* at 630. Similarly, in *Weeks v. United States*, the Court held that the warrantless search and seizure of articles in the home of a man whom had just been arrested violated the Fourth Amendment. *Weeks v. United States*, 232 U.S. 383, 398-99 (1914) *overruled by* *Mapp v. Ohio*, 367 U.S. 206 (1961). After the defendant's arrest, police officers went to his house, obtained a key from his neighbor, entered his room and searched it, seizing various papers and articles that were used against him at trial. *Id.* at 386-87. Following its reasoning in *Boyd*, the Supreme Court in 1962 held that the Fourth Amendment did not apply in the absence of a physical intrusion into a "constitutionally protected area" such as a house. *See Lanza v. New York*, 370 U.S. 139, 142-43 (1962) (distinguishing a jail cell from other constitutionally protected areas). Perhaps the most significant example of the Court's property rights/trespass approach to the Fourth Amendment is set forth in *Olmstead v. United States*. *Olmstead v. United States*, 277 U.S. 438, 469 (1928), *overruled by* *Katz v. United States*, 389 U.S. 347 (1967). *See infra* notes 56, 58-63 and accompanying text (providing a discussion of *Olmstead*); *see infra* notes 64-67 and accompanying text (providing an overview of *Katz*).

56. *Olmstead*, 277 U.S. at 438.

57. U.S. CONST. amend. IV.

58. *Olmstead*, 277 U.S. at 465. "The language of the Amendment cannot be extended and expanded to include telephone wires The intervening wires are not part of his house or office any more than are the highways along which they are stretched." *Id.*

59. *Id.* at 455 (citing the National Prohibition Act).

60. *Id.* at 455-57. The prosecution claimed that the defendants unlawfully possessed, transported, imported, and sold intoxicating liquors. *Id.* at 455. The evidence demonstrated a

defendants argued that wiretapping violated their Fourth Amendment rights to be free from governmental intrusion.⁶¹ However, the Court decided, after reviewing prior case law,⁶² to decline extending the protections of the Fourth Amendment to include anything other than an official search and seizure of the person, papers, tangible material effects, or an actual physical invasion of the defendant's house.⁶³

The Court upheld its ruling in *Olmstead* until 1967, when it broadened the Fourth Amendment protections in *Katz v. United States* to include searches of people as well as places.⁶⁴ Justice Harlan's concurring opinion set forth a two-part test used to determine whether a search or seizure is reasonable.⁶⁵ First, the court must decide whether the individual had a subjective expectation of privacy.⁶⁶ If the answer is yes, the court must then determine whether society objectively recognizes that individual's expectation of privacy.⁶⁷ One manner for

conspiracy involving at least fifty persons, with aggregate sales ranging from \$176,000 to \$2,000,000. *Id.* at 456. The information leading to the discovery of the conspiracy was primarily obtained through the unwarranted interception of telephone conversations by four federal prohibition officers. *Id.* The wiretaps were inserted without trespass to any property of the defendants. *Id.* at 457.

61. *Id.* at 455.

62. The Court relied, in part, on *Boyd v. United States*, as well as *Weeks v. United States* in reaching its decision. *Id.* at 458-60; see also *supra* note 55 (discussing *Boyd* and *Weeks*).

63. *Olmstead*, 277 U.S. at 466.

The Amendment itself shows that the search is to be of material things—the person, the house, his papers, or his effects The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only.

Id. at 464. Justice Brandeis dissented, arguing that new technology required an expansion of Fourth Amendment protection principles. *Id.* at 473 (Brandeis, J., dissenting). Arguing that electronic surveillance should require Fourth Amendment protection, Justice Brandeis stated, “‘time works changes, brings into existence new conditions and purposes.’ Subtler and more far-reaching means of invading privacy have become available to the Government.” *Id.* (Brandeis, J., dissenting).

64. *Katz v. United States*, 389 U.S. 347 (1967). While the majority opinion rejected the physical trespass doctrine, it expanded Fourth Amendment privacy protections to almost anything a person seeks to preserve as private, but it did not offer a new test for Fourth Amendment analysis. *Id.* at 351-52. In language proving to be very important in post-*Katz* cases, Justice Stewart explained that “[w]hat 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 [such as a public telephone booth] may be constitutionally protected.” *Id.* (citations omitted).

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

66. *Id.* (Harlan, J., concurring).

67. *Id.* (Harlan, J., concurring). In his concurring opinion in *Katz v. United States*, Justice Harlan stated, “[m]y understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’” *Id.* (Harlan, J., concurring).

an individual to establish that a subjective expectation of privacy exists is to demonstrate that uninvited people will not intrude,⁶⁸ which typically is a question of fact.⁶⁹ Whether society recognizes the individual's expectation of privacy is a question of law to be determined after examining all the surrounding circumstances.⁷⁰

B. Electronic Surveillance, Warrantless Searches, and the So-Called National Security Exception

Original Fourth Amendment analysis focused on privacy as a property interest, limiting the Fourth Amendment protections to physical searches of a person's property.⁷¹ In *Katz v. United States*, the Supreme Court extended those protections to non-physical, electronic surveillance, even when no physical intrusion occurred.⁷² The Court held that the Fourth Amendment applied to people and not places, and it

68. *United States v. Lyons*, 706 F.2d 321, 326 (D.C. Cir. 1983); see Freund, *supra* note 28, at 201-03 (discussing the subjective expectation of privacy).

69. *United States v. McBean*, 861 F.2d 1570, 1573 (11th Cir. 1988).

70. See *id.* at 1573 n.7; see also Freund, *supra* note 28, at 203-04. To answer this question, a court must examine the incident and balance the "individual's legitimate expectation of privacy and . . . the government's need for effective law enforcement." Freund, *supra* note 28, at 204. The Fourth Amendment also protects individuals from unreasonable government seizures of persons and property. See U.S. CONST. amend. IV; *supra* notes 40-63 and accompanying text (discussing Fourth Amendment application, including the warrant and probable cause requirements). If, in view of all circumstances surrounding the incident, a reasonable person believes he or she is not free to leave an encounter with a government official, that person has been seized. *Michigan v. Chesternut*, 486 U.S. 567, 573 (1988); *United States v. Mendenhall*, 446 U.S. 544, 554 (1980); see *supra* notes 32-33 and accompanying text (discussing reasonable detention when police have no warrant); see also *Florida v. Bostick*, 501 U.S. 429, 432 (1991) (finding that a court must consider all circumstances surrounding an occurrence in determining if a reasonable person would believe he had been seized); *INS v. Delgado*, 466 U.S. 210, 218-19 (1984) (finding no seizure of employees during factory survey despite presence of INS agents at exits because mere probability of being questioned upon leaving did not reasonably result in conclusion that the employees were not ultimately free to leave). However, when government intrusion meaningfully interferes with an individual's possessory interest, a property seizure has occurred. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (finding seizure when DEA agent asserted dominion and control over a package at a Federal Express office). But see *Arizona v. Hicks*, 480 U.S. 321, 324-25 (1987) (finding no seizure when police recorded serial numbers of stereo equipment because no meaningful interference with defendant's possessory interest in either numbers recorded or stereo).

71. See *supra* notes 40-63 and accompanying text (providing an overview of early Fourth Amendment analysis).

72. *Katz*, 389 U.S. at 359. The defendant was convicted of transmitting wagering information by telephone from one state to another in violation of a federal statute, primarily based on evidence obtained when the FBI listened to his calls from a public telephone booth. *Id.* at 348. FBI agents had attached an electronic listening and recording device to the outside of a public telephone booth from which the defendant was known to make calls. *Id.* The Court of Appeals previously affirmed the defendant's conviction because there had been no physical invasion into any property occupied by the defendant. *Id.* at 348-49.

determined that a government agent need not physically intrude into a specific enclosure to violate the Fourth Amendment.⁷³

In *Katz*, the Government argued that the Court should create a special warrant exception for electronic surveillance.⁷⁴ The Court refused, stating that whenever possible a warrant must be obtained and be based on a neutral predetermination of probable cause.⁷⁵ In dicta, however, the Court recognized the possibility that in matters of national security prior authorization for electronic surveillance may not always be required,⁷⁶ limiting its decision to issues of domestic criminal surveillance only.⁷⁷

The Court finally addressed the relationship between issues of domestic national security and electronic surveillance in 1972, in *United States v. United States District Court* (hereinafter "*Keith*").⁷⁸ In *Keith*, the defendants were charged with conspiracy to destroy government property.⁷⁹ Prior to trial, the defendants moved to compel the government to disclose certain electronic surveillance information, which was allegedly obtained through illegal means.⁸⁰ Although the

73. *Id.* at 353. In his concurrence, Justice Harlan stated that after considering modern-day technology, the physical trespass analysis of the past was "bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion." *Id.* at 362 (Harlan, J., concurring). The Court stated that a showing of probable cause after the search was completed would not satisfy the Fourth Amendment. *Id.* at 358. Writing for the majority, Justice Stewart stated, "[o]mission 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." *Id.* (citations omitted).

74. *Id.*

75. *Id.*

76. *Id.* at 358 n.23. "Whether safeguards other than prior authorization . . . would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." *Id.*

77. *See id.* Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (OCCSSA) in response to the holding in *Katz*. *See Banks & Bowman, supra* note 28, at 48 (noting that OCCSSA established guidelines for judicial authorization of electronic surveillance in the investigation of specific, enumerated crimes); *see infra* Part II.D.2 (discussing the enactment and provisions of OCCSSA).

78. *United States v. United States District Court*, 407 U.S. 297, 299 (1972) [hereinafter *Keith*]. *Keith* was the federal district court judge who heard the case. Brown & Cinquegrano, *supra* note 33, at 115. Subsequently, commentators have typically referred to this case as the "*Keith*" decision. *Id.*

79. The defendants were charged with violating 18 U.S.C. § 371. *Keith*, 407 U.S. at 299. One defendant was charged with the dynamite bombing of a Central Intelligence Agency office in Ann Arbor, Michigan. *Id.*

80. *Id.* at 299-300. The government acknowledged that the Attorney General had approved certain wiretaps to gather intelligence information necessary to protect the nation from domestic terrorist attacks. *Id.* at 300.

government argued that the surveillance was reasonable as an exercise of the executive branch's power to protect national security,⁸¹ the district court held that the surveillance violated the defendant's Fourth Amendment rights.⁸²

On appeal, the Supreme Court held that warrantless electronic surveillance of a domestic organization with no alleged connection to a foreign government constituted a breach of Fourth Amendment protections.⁸³ The Court emphasized that, while requiring a warrant for electronic surveillance of domestic organizations places an added burden upon the Attorney General, the inconvenience serves to protect constitutional values.⁸⁴ The Court recognized that, in cases of national security, the power of the executive branch to engage in surveillance should be stronger.⁸⁵ However, the Court noted that waiving the warrant requirement in domestic security cases could lead to broad abuses by the executive, greatly interfering with the needs of individuals for "privacy and the free expression."⁸⁶ The Court did not discuss

81. The government relied on OCCSSA, 18 U.S.C. § 2511(3) (1968) (repealed 1978), in making its argument. *Keith*, 407 U.S. at 303. Section 2511(3) states, in part:

Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack . . . [or] to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.

18 U.S.C. § 2511(3) (1968) (repealed 1978); *see infra* Part II.C.2 (discussing the statute and its enactment). The Supreme Court, in *Keith*, stated that this language only affirms the powers already vested in the President by the Constitution and is neutral regarding the use of the President's electronic surveillance power. *Keith*, 407 U.S. at 303.

82. *Keith*, 407 U.S. at 301.

83. *See id.* at 321-22, 324. The Court emphasized that this case "involves only the domestic aspects of national security . . . express[ing] no opinion as to [] the issues which may be involved with respect to activities of foreign powers or their agents." *Id.* at 322. The Court further specified that the decision did not rest on any section of OCCSSA, nor did the Act try to "define or delineate the powers of the President to meet domestic threats to the national security." *Id.*; *see Banks & Bowman, supra* note 28, at 50 (discussing Justice Powell's opinion that it was reasonable to protect the government from subterfuge through the use of electronic surveillance).

84. *Keith*, 407 U.S. at 321. "A prior warrant establishes presumptive validity of the surveillance and will minimize the burden of justification in post-surveillance judicial review." *Id.*

85. *Id.* at 313.

86. *See id.* at 313-15. Eerily foreshadowing Congress' present expansion of electronic surveillance powers, Justice Powell stated,

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.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.

whether it would reach the same conclusion for cases involving warrantless electronic surveillance in foreign intelligence gathering or domestic organizations with a foreign connection,⁸⁷ leaving open the possibility of different Fourth Amendment standards for national security investigations involving foreign organizations.⁸⁸

Because the same techniques are used in gathering intelligence for national security purposes that are used in enforcing domestic criminal law, Fourth Amendment concerns arise.⁸⁹ It is important to recognize that a distinction exists between the warrant requirement for criminal investigations, and the warrant requirement for intelligence gathering.⁹⁰ Whether Fourth Amendment protections should be applied to foreign intelligence gathering, or a warrant exception for this should be recognized, remains unresolved by the Supreme Court.⁹¹ However, several federal appellate courts have addressed this issue, with mixed results.⁹² In order to fully understand the role of the current national

Id. at 314.

87. *See id.* at 321-22.

We emphasize, before concluding this opinion, the scope of our decision . . . this case involves only the domestic aspects of national security. 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.

Id. at 321-22.

88. *Id.* at 322; *see also* Banks & Bowman, *supra* note 28, at 52 (reviewing the *Keith* decision). Similar to Congress' enactment of OCCSSA after the *Katz* decision, after *Keith*, Congress enacted the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. §§ 1801-1811. *See* Robert A. Dawson, *Shifting the Balance: The D.C. Circuit and the Foreign Intelligence Surveillance Act of 1978*, 61 GEO. WASH. L. REV. 1380, 1382-97 (1993) (reviewing the enactment of FISA and subsequent court decisions); *infra* Part II.D.3 (providing a complete discussion of FISA and its application); *see also infra* notes 128-37 and accompanying text (discussing Congress' enactment of OCCSSA).

89. *See* Banks & Bowman, *supra* note 28, at 4. "While secrecy may be an essential ingredient of successful national security surveillance, increasingly sophisticated forms of electronic eavesdropping may also threaten personal freedoms." *Id.*

90. *Id.* at 5-6. "It is neither the objective nor the likely result that the target of a foreign intelligence . . . search will be criminally prosecuted." *Id.* at 5. *See Keith*, 407 U.S. at 322 (recognizing that traditional criminal law warrant requirements may not apply in domestic security surveillance).

91. *See* Banks & Bowman, *supra* note 28, at 91. Several circuit courts have held that FISA is a "constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information." *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984).

92. *See United States v. Butenko*, 494 F.2d 593, 602 (3d Cir. 1974) (en banc) (holding electronic surveillance conducted without a warrant was constitutional, even though the primary purpose of the surveillance was to obtain foreign intelligence information); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973) (holding that unwarranted electronic surveillance for foreign intelligence purposes was constitutional when an American citizen was incidentally overheard); *see also United States v. Cavanagh*, 807 F.2d 787, 790-91 (9th Cir. 1987) (holding that when

security legislation, it is necessary to look at its historical development.⁹³

C. Early American Intelligence Activity

In 1775, the Continental Congress created the Committee for Secret Correspondence, authorizing the first official intelligence activities of the United States government, which led to the establishment of the national security laws.⁹⁴ Congress subsequently enacted legislation in 1777 making espionage a capital offense.⁹⁵ As the nation's first President, George Washington took personal responsibility for foreign intelligence and was successful in pressuring Congress to establish a fund for these operations.⁹⁶

balancing the government's interests in pursuing intelligence activity against the individual's freedom from governmental intrusion, FISA warrants satisfy Fourth Amendment concerns); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987) (stating that FISA safeguards provide sufficient protection under the Fourth Amendment for FISA issued warrants); *infra* Part II.D.3 (providing a discussion of FISA requirements). *But see* *Zweibon v. Mitchell*, 516 F.2d 594, 613-14 (D.C. Cir. 1975), *aff'd in part, rev'd in part*, 606 F. 2d 1172 (D.C. Cir. 1979) (holding narrowly that absent exigent circumstances, a warrant must be obtained before conducting electronic surveillance of domestic organizations with no foreign connection, rejecting arguments by the government that any national security exception to the warrant requirement would be constitutionally permissible, and refusing to broaden its holding to include all foreign security surveillance).

93. *See infra* Part II.C-E (discussing the development of national security legislation).

94. Banks & Bowman, *supra* note 28, at 10-11 (providing a history of national security law from 1775 to the Antiterrorism Effective Death Penalty Act of 1996). The five member congressional committee represented the first official American intelligence activity, classifying communications with foreign countries by withholding the names of persons with whom they worked and corresponded. *Id.* at 9 n.57-58. National security law focuses on securing the safety of American citizens, protecting the country, in part, from espionage, terrorist attacks, and the threat of government overthrow. *See infra* Part II.D (discussing modern national security law).

95. Banks & Bowman, *supra* note 28, at 12. Espionage is defined as "the act or practice of spying or of using spies to obtain secret information, as about another government or a business competitor." AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (4th ed. 2000). The first espionage legislation was passed after Dr. Benjamin Church, a spy for the British army during the Revolutionary War, was caught and tried by court martial. Banks & Bowman, *supra* note 28, at 11-12. At the time of his trial, espionage was not a crime for civilians. *See id.* at 12. After that trial, espionage became a capital offense for all non-Americans found to be spying on the United States. *Id.* Congress amended the legislation in 1778 to include anyone residing in the United States, including American citizens, who assisted another country in killing or capturing loyal United States citizens. *Id.*

96. Banks & Bowman, *supra* note 28, at 15. After the Revolutionary War, Americans distrusted executive power, but they realized that a strong Executive Branch was necessary. *Id.* at 14. Thus, the founders purposefully created a system of government with shared powers between the Executive and Legislative branches. *Id.* President Washington, however, skilled in intelligence gathering, took personal responsibility for this important government function, and Congress did not attempt to limit his ability to do so. *Id.* at 15.

President Thomas Jefferson continued to exercise the broad executive control over intelligence gathering, authorizing a wide spectrum of covert actions to protect national security by guarding against foreign infiltration.⁹⁷ Subsequent presidents continued to assert broad executive control over intelligence matters and national security concerns well into the twentieth century.⁹⁸ During this time, Congress continued to authorize such funds, leaving the details of intelligence matters in the hands of the executive branch.⁹⁹

D. Legislation and National Security Actions from 1917 to the Present

Modern-day use of wiretapping for national security purposes began at the start of the twentieth century with limited Congressional oversight and has evolved significantly since that time.¹⁰⁰ In the mid-twentieth century, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act (OCCSSA), which provided guidelines for electronic surveillance in criminal investigations.¹⁰¹ Ten years later, Congress enacted the Foreign Intelligence Surveillance Act of 1978 (FISA), which clarified the extent to which the government could engage in wiretapping for national security purposes.¹⁰² As a reaction to the 1995

97. *Id.* at 16. During President John Adams' term in office, Congress enacted the Alien and Sedition laws, allowing for the extra-judicial deportation of legal resident aliens whom the administration considered to be a security threat. *Id.*; see Alien Enemies Act, 1 Stat. 577 (1798) (expired), and 1 Stat. 596 (1798) (expired); Alien Act, 1 Stat. 570 (1798) (expired); Naturalization Act, 1 Stat. 566 (1798) (expired); David B. Kopel & Joseph Olson, *Preventing a Reign of Terror: Civil Liberties Implications of Terrorism Legislation*, 21 OKLA. CITY U. L. REV. 247, 252-53 (1996) (discussing early presidential attempts to provide national security, including the Alien and Sedition laws signed by President Adams). These Acts were never uniformly enforced, and they were allowed to expire during Thomas Jefferson's presidency. Kopel & Olson, *supra*, at 253.

98. Banks & Bowman, *supra* note 28, at 17-18. For example, President Lincoln mobilized state militias, established blockades against rebellious states and suspended writs of habeas corpus. *Id.* at 17. "Congress consistently deferred to the president when he withheld secret official records, . . . employed secret agents, . . . ransomed hostages, and even when he engaged in covert operations." *Id.* at 18. For example, in 1936, President Roosevelt directed FBI field agents to gather information regarding all activities by communists, fascists, and other organizations with potential plans to overthrow the United States government. *Id.* at 26-27.

99. *Id.* at 17-29. "It was common for Congress to withdraw requests for official records when the president balked at providing them and to appropriate funds for secret purposes when the president requested them." *Id.* at 18. Private citizens were not concerned by this practice, because "the nature of intelligence activities rarely touched [their] private lives." *Id.* at 17.

100. See *infra* Part II.D.1 (providing an overview of early congressional oversight of electronic surveillance). See generally Banks & Bowman, *supra* note 28, at 19-20.

101. See *infra* Part II.D.2 (discussing the Omnibus Crime Control and Safe Streets Act of 1968).

102. See *infra* Part II.D.3 (discussing the Foreign Intelligence Surveillance Act of 1978).

bombing of the Federal Building in Oklahoma City, the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) was enacted.¹⁰³

In the early 1900s, threats to national security evolved simultaneously with the increasing technological and political sophistication of various nations.¹⁰⁴ In 1915, for example, on the brink of World War I, President Wilson placed German and Austro-Hungarian delegations to the United States under surveillance.¹⁰⁵ Furthermore, the President authorized the United States Secret Service to install wiretaps on these delegations, which provided enough information regarding potential sabotage activities to expel the German Naval Attaché to the United States.¹⁰⁶ Over the next two years, similar events led to the enactment of the Espionage Act of 1917.¹⁰⁷ This Act gave the government greater surveillance authority and the ability to censor and restrict the right of assembly for certain radical groups that were considered a threat to the interests of the United States during World War I.¹⁰⁸

At the end of World War I, concerns regarding an imminent attempt to overthrow the United States government continued to guide U.S. Army intelligence, resulting in raids on suspected radical groups and continued surveillance of citizens.¹⁰⁹ Domestic intelligence remained the primary responsibility of the executive branch, carried forth by members of the Justice Department's young Federal Bureau of

103. See *infra* Part II.D.4 (providing an overview of the Antiterrorism and Effective Death Penalty Act of 1996).

104. See Banks & Bowman, *supra* note 28, at 19. World War I loomed on the horizon, and Germany became a threat to national security, planning to invade the United States and sending German officers to assess beachhead sights. *Id.* at 19-20. Germany had made technological advances in torpedoes, torpedo-boat destroyers, and newly invented wireless telegraphs. G.J.A. O'TOOLE, HONORABLE TREACHERY: A HISTORY OF U.S. INTELLIGENCE, ESPIONAGE, AND COVERT ACTION FROM THE AMERICAN REVOLUTION TO THE CIA 206 (1991).

105. See Banks & Bowman, *supra* note 28, at 19-20. The German Naval Attaché was one of the key German officers involved in sabotage activities. *Id.* at 20. Discoveries of other German activities led to many changes in American national security plans. See *id.* at 21-24.

106. *Id.* at 20.

107. Espionage Act of 1917, Pub. L. No. 65-24, 40 Stat. 217 (1919), available at <http://www.staff.uiuc.edu/~rcunning/espact.htm>.

108. Banks & Bowman, *supra* note 28, at 22. The Act gave the government greater authority to "confiscate property, wiretap, search and seize private property, censure writings, open mail and restrict the right of assembly." *Id.*; see also O'TOOLE, *supra* note 104, at 272-73 (noting that the Act was the most brutal attack on free speech since the Sedition Act of 1798).

109. Banks & Bowman, *supra* note 28, at 24. The FBI authorized the American Protective League (APL), an army of unpaid volunteers, to act without police powers and root out draft dodgers and other radicals believed to be engaged in dissident activities against the United States. *Id.* at 23. Communists and communist labor parties across the United States were targeted, and thousands were arrested without probable cause. *Id.* at 24.

Investigations.¹¹⁰ Today, FBI investigations are typically within the discretion of the Attorney General and limited to criminal investigations.¹¹¹

Eventually, responsibility for domestic security was expanded to include the Department of Defense and the Central Intelligence Agency.¹¹² The FBI was to be directed by the Attorney General.¹¹³ However, President Roosevelt bypassed the Attorney General and personally directed the FBI regarding many intelligence investigations.¹¹⁴ Following Roosevelt's instructions, the FBI established files on private citizens regarding their private lives and began investigations for intelligence gathering purposes only, even without evidence of criminal activity on the part of the person being watched.¹¹⁵ As technology developed, the role of wiretapping in intelligence gathering investigations became both increasingly important and extreme.¹¹⁶

1. Wiretapping and Early Congressional Oversight of Electronic Surveillance

Law enforcement officials utilized telephone wiretaps in "exceptional cases" throughout the 1930s for intelligence investigations of substantial and serious crimes by ordinary American citizens.¹¹⁷ Such

110. *Id.* at 26. The FBI was established during President Roosevelt's presidency in 1908. *See History of the FBI—Origins, 1908-1910*, at <http://www.fbi.gov/fbinbrief/historic/history/origins.htm> (last modified June 14, 2001). The Central Intelligence Agency was created in 1947 with the signing of the National Security Act by President Truman, charging the new agency with coordinating the nation's intelligence activities. *See About the CIA*, at <http://www.cia.gov/cia/information/info.html> (last modified Feb. 4, 2002).

111. *See Banks & Bowman, supra* note 28, at 26.

112. *Id.* What is generally thought of as the modern era of the FBI began with J. Edgar Hoover's appointment in 1924. *Id.*

113. "Operational policy for the Bureau, and the new Director, limited the FBI to investigations operating under the direction of the Attorney General for the purpose of gathering facts concerning violations of federal laws." *Id.* These principles "remain the essence of FBI investigative policy today." *Id.*

114. *See id.* at 26-27. Technically, intelligence investigations were outside the scope of the FBI. *Id.* at 27. According to a 1976 Senate Report, Roosevelt ordered the FBI to "obtain from all possible sources information concerning subversive activities conducted in the United States . . . advocating the overthrow or replacement of the government of the United States by illegal methods." S. REP. NO. 94-755, at 560-62 (1976).

115. Banks & Bowman, *supra* note 28, at 26-27.

116. *See id.* at 27. "The executive orders upon which the Bureau based its intelligence activity in the decade before World War II were vague and conflicting . . . using words like 'subversion' . . . and permitting the investigation of 'potential' crimes." *Id.* (quoting S. REP. NO. 94-755, at 24 (1976)).

117. Banks & Bowman, *supra* note 28, at 27.

investigations were allowed as long as the activity of the person was criminal in the eyes of the FBI Bureau Chief and the Attorney General.¹¹⁸ The head of the FBI or the Attorney General authorized these wiretaps with little or no judicial oversight.¹¹⁹ In 1934, realizing the potential threat to personal privacy established by wiretapping, Congress enacted the Federal Communications Act,¹²⁰ placing the first restrictions on wiretapping.¹²¹ This Act made it a crime for any person to divulge the contents of wire or radio to any person other than an authorized receiver.¹²² The Justice Department interpreted this legislation to include non-law enforcement wiretaps only and basically ignored the legislation.¹²³

In 1940, President Roosevelt authorized the Attorney General to approve electronic surveillance of anyone considered to be a threat to national security.¹²⁴ By 1954, J. Edgar Hoover instructed FBI agents to enter private property and install electronic surveillance devices as national security interests required.¹²⁵ For example, surveillance was employed against suspected communists during the Cold War and the McCarthy era.¹²⁶ The expansive nature of governmental intelligence

118. *Id.*

119. *Id.*; see S. REP. NO. 95-604, at 8 (1977), reprinted in 1978 U.S.C.A.A.N. 3904, 3909; see also Donna M. Gaudet, *Constitutional Law—Fourth Amendment—Electronic Surveillance Authorized Under the Foreign Intelligence Surveillance Act Does Not Violate the Fourth Amendment*, United States v. Posey, 864 F.2d 1487 (9th Cir. 1989), 14 SUFFOLK TRANSNAT'L L.J. 231, 233-36 (1990).

Historically, the President of the United States has assumed the power to authorize electronic surveillance without prior judicial approval where national security is at risk The primary focus of electronic surveillance in foreign intelligence investigations is to intercept and stop the flow of technological information that could potentially jeopardize national security.

Gaudet, *supra*, at 235-36.

120. Federal Communications Act, ch. 652, 48 Stat. 1103 (1934), available at <http://showcase.netins.net/web/akline/1934act.htm>. The FCA was created “[f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio . . . [and] for the purpose of national defense” *Id.*

121. Banks & Bowman, *supra* note 28, at 28. “[T]he Justice Department interpreted the Federal Communications Act . . . as prohibiting only the interception and divulgence of the contents of wiretaps conducted outside the authority of Federal law enforcement.” *Id.*

122. *Id.*

123. *Id.*

124. *Id.* President Roosevelt specifically authorized electronic surveillance where “‘grave matters involving defense of the nation’ were at stake.” *Id.* (citing S. REP. NO. 95-604, at 10 (1977), reprinted in 1978 U.S.C.A.A.N. 3904, 3911).

125. *Id.* at 28-29. Approval by the Attorney General was not required in these situations. *Id.* at 28.

126. See Debora K. Kristensen, *Finding the Right Balance: American Civil Liberties in Time of War*, ADVOCATE (IDAHO), Dec. 2001, at 20, 22.

gathering and surveillance continued through the 1960s, when Congress took a more active role in national security issues, focusing on intelligence matters and privacy issues.¹²⁷

2. Title III of the Omnibus Crime Control and Safe Streets Act of 1968: Domestic Criminal Wiretapping

In 1968, Congress enacted Title III of the OCCSSA,¹²⁸ a comprehensive statute covering domestic wire and electronic surveillance in criminal cases.¹²⁹ Congress enacted this legislation in order to regulate the interception of wire, oral, and electronic communications¹³⁰ of anyone law enforcement suspected of criminal

127. Banks & Bowman, *supra* note 28, at 30-31. In 1975, President Ford created the Commission on CIA Activities Within the United States, known as the Rockefeller Commission, to investigate whether CIA activities violated the rights of private citizens through a pattern of domestic activity. *Id.* at 32-33. This investigation led to a complete study of the propriety of intelligence activities. *Id.* Also in 1975, President Ford created the Church Committee, or the Select Committee to Study Governmental Operations With Respect to Intelligence Activities, to conduct an inquiry into the intelligence system as a whole. *Id.* at 33. The Church Committee found that intelligence efforts violated the Constitution, and that the solution was to have Congress adopt rules for intelligence activities. *Id.* at 33-34.

128. See OCCSSA, 18 U.S.C. §§ 2510-2522 (2000). OCCSSA is frequently referred to as Title III or the Federal Wiretap Act. *Id.* However, for purposes of this Comment, it will be referenced as OCCSSA, in order to distinguish it from Title III of the USA PATRIOT Act. In 2000, none of the 1,190 federal wiretap requests in criminal cases were denied by federal or state courts. Center for Democracy & Technology, *The Nature and Scope of Governmental Electronic Surveillance Activity* (Sept. 2001), at http://www.cdt.org/wiretap/wiretap_overview.html. Seventy-five percent of these wiretaps were for drug related crimes. *Id.* The wiretaps intercepted approximately 2.1 million conversations from 196 persons. *Id.* The longest running wiretap lasted 308 days. *Id.* Statistics show that twenty-three percent of conversations intercepted were incriminating. *Id.*

129. See OCCSSA §§ 2510-2522. Wiretaps may be authorized for any of the more than 100 offenses listed in § 2516 of OCCSSA, including bribery, obstruction of criminal investigations, interstate transportation of stolen property, and sexual exploitation of children, to name a few. 18 U.S.C. § 2516(1)(C), *amended by* Pub. L. No. 107-56, Title II, § 202, 115 Stat. 278. See also Christian David Hammel Schultz, *Unrestricted Federal Agent: "Carnivore" and the Need to Revise the Pen Register Statute*, 76 NOTRE DAME L. REV. 1215, 1217, 1232 (2001) (discussing OCCSSA and its relationship to CARNIVORE, an "electronic surveillance system that monitors a targeted user's e-mail, web browsing, and file transfer activity").

130. Scott D. Joiner, *Electronic Surveillance*, 89 GEO. L.J. 1163 (2001). OCCSSA defines wire communication as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection . . . or communications affecting interstate or foreign commerce." 18 U.S.C. § 2510(1) (2000), *amended by* Pub. L. 107-56, Title II, § 209(1)(A), 115 Stat. 283.

Oral communication is defined as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but . . . does not include any electronic communication." 18 U.S.C. § 2510(2).

Electronic communication is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic,

activity, recognizing the threat to privacy rights that results from the unrestricted use of such surveillance.¹³¹ The OCCSSA mandates that law enforcement officials receive authorization from the Attorney General before applying for a court order to intercept wire or oral communications.¹³² However, any government attorney may grant authorization for electronic communication interception.¹³³

Once the government agent grants authorization, application may be made to a judge, who can enter an order authorizing the intercept only after determining that probable cause exists regarding the individual involved.¹³⁴ When probable cause exists, the judge may issue the order, which must specify the identity of the person targeted by the surveillance as well as the facilities to be used and the time period for the interception.¹³⁵ Furthermore, before issuing the order, the court must find that normal investigative techniques have failed, appear unlikely to succeed, or would be too dangerous for law enforcement.¹³⁶

photoelectronic or photooptical system that affects interstate or foreign commerce” 18 U.S.C. § 2510(12).

131. Joiner, *supra* note 130, at 1163-64. The only people authorized to approve the submission of a request for wire or oral communication surveillance are the United States Attorney General or a specially designated Assistant or Deputy Assistant Attorney General in the Criminal Division. *Id.* at 1165.

132. Joiner, *supra* note 130, at 1165; *see* 18 U.S.C. § 2516 (provisions governing authorization of application for surveillance); 18 U.S.C. § 2518 (provisions governing contents of application, order, and issuance of order by court). For a wiretap to be granted under OCCSSA, there must be probable cause to believe that a crime has been, is being, or is about to be committed. 18 U.S.C. § 2518; *see also* Center for Democracy & Technology, *supra* note 128.

133. Joiner, *supra* note 130, at 1166. “The application must identify the applicant and the person authorizing it and, once authorized, is submitted to a court to secure the requisite court order.” *Id.* Authorization for electronic communication may be granted for “any federal felony,” as opposed to authorization for wire or oral communications. 18 U.S.C. § 2516(3).

134. Schultz, *supra* note 129, at 1233-34; *see* 18 U.S.C. § 2518(4). The judge or magistrate must also consider “the relationship between the communication to be intercepted and the accused offense, and the appropriateness of the facilities to be targeted or used to intercept the communication.” Schultz, *supra* note 129, at 1234; *see* 18 U.S.C. § 2518(1). Probable cause is the level of suspicion required to justify certain governmental intrusions upon protected Fourth Amendment interests. *See Ornelas v. United States*, 517 U.S. 690, 696 (1996).

135. Schultz, *supra* note 129, at 1233-34. “An order authorizing electronic surveillance shall be executed ‘as soon as practicable,’” and must “terminate upon attainment of the authorized objective.” 18 U.S.C. § 2518(5). Surveillance cannot last more than thirty days without an extension. 18 U.S.C. § 2518(5).

136. 18 U.S.C. § 2518; Joiner, *supra* note 130, at 1169. OCCSSA imposes four post-authorization duties upon those acting under an electronic surveillance order. *See* 18 U.S.C. § 2518. First, the police must minimize the interception of communications outside the scope of the authorization and order, and this effort must be objectively reasonable in light of the circumstances confronting the interceptor. *Id.* § 2518(5). Second, the court must seal the application for an OCCSSA order and the order itself immediately after the specified surveillance period in order to protect confidentiality and to prevent tampering. *Id.* § 2518(8). Third, an “inventory” must be issued to those persons named in the order, and possibly to other persons

Ten years after the enactment of OCCSSA, Congress enacted the Foreign Intelligence Surveillance Act of 1978, authorizing electronic surveillance for foreign intelligence purposes.¹³⁷

3. The Foreign Intelligence Surveillance Act of 1978: Wiretapping and Foreign Intelligence Surveillance

As OCCSSA authorizes electronic surveillance only in criminal cases,¹³⁸ Congress determined that similar legislation authorizing electronic surveillance for foreign intelligence gathering purposes was necessary.¹³⁹ In 1978, President Jimmy Carter signed into law the FISA.¹⁴⁰ FISA allows wiretapping of aliens and citizens in the United

whose conversations have been intercepted. *Id.* § 2518(8)(d). Fourth, intercepted communications may be lawfully used only in three situations: (1) disclosure between law enforcement officers when "appropriate"; (2) the information intercepted may be used in the performance of the law enforcement officer's official duties; and (3) the contents of an intercepted communication may be disclosed by any person while giving testimony "in any proceeding held under the authority of the United States or of any State." 18 U.S.C. § 2517(3).

137. See *infra* Part III.B.3 (discussing the enactment of FISA).

138. OCCSSA, 18 U.S.C. §§ 2510–2522 (2000).

139. See Louis A. Chiarella & Michael A. Newton, "So Judge, How do I get that FISA Warrant?": *The Policy and Procedure for Conducting Electronic Surveillance*, ARMY LAW, Oct. 1997, at 25, 25.

The subject of a law enforcement investigation eventually learns of or knows about any searches and surveillance. . . . [but] the 'subject' of [foreign intelligence gathering] will not learn of searches and surveillance conducted, except in those exceptional instances where the Attorney General later approves the use of the collected information as criminal evidence.

Id. at 27; Ronald J. Sievert, *Meeting the Twenty-First Century Terrorist Threat Within the Scope of Twentieth Century Constitutional Law*, 37 HOUS. L. REV. 1421, 1437 (2000) (providing a hypothetical national security incident and potential responses using FISA and other protection measures).

140. FISA, 50 U.S.C. §§ 1801–1863 (1994 & Supp. V 1999). FISA authorizes the Attorney General to approve applications for warrants to conduct electronic surveillance or physical searches within the United States for the purposes of foreign intelligence if the target is a foreign power or an agent of a foreign power. *Id.* § 1801(e). Foreign intelligence information means:

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other rave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

States when there is probable cause to believe that the target of the wiretap is a member of a foreign terrorist group or an agent of a foreign power.¹⁴¹ FISA seeks to deter espionage within the United States by a foreign government or component thereof, by any entity that a foreign government acknowledges it controls and directs, and by any group engaged in international terrorism.¹⁴²

Designed to maintain a balance between national security interests and the privacy interests of United States citizens,¹⁴³ FISA requires that a designated government official apply for electronic surveillance warrants under 50 U.S.C. § 1804¹⁴⁴ and for physical searches under section 1823.¹⁴⁵ Applications for FISA warrants are made to a specially authorized FISA court, consisting of seven United States District Court

Id. In part, FISA was passed as a response to *Keith*. See *supra* note 88; Sievert, *supra* note 139, at 1436-37; see also Banks & Bowman, *supra* note 28, at 76 (discussing FISA surveillance measures); Gerald H. Robinson, *We're Listening! Electronic Eavesdropping, FISA, and the Secret Court*, 36 WILLAMETTE L. REV. 51 (2000) (describing FISA and the FISA court's role in national security investigations).

141. 50 U.S.C. §§ 1801-1811.

142. *Id.* §§ 1804, 1823; see Robinson, *supra* note 140, at 56-57. Robinson states, "[c]learly more than one evil spirit lurks in FISA's definitional language, which is vague and subject to elastic interpretation." *Id.* at 56. FISA defines foreign power as "a foreign government or a component thereof, whether or not recognized by the United States, as well as a 'faction' of a foreign nation or nations, not substantially composed of United States persons." *Id.* Foreign Intelligence Information includes "information that relates to . . . the United States' ability to protect against an 'actual or potential attack or other grave hostile acts of a foreign power or . . . agent,' 'sabotage or international terrorism . . .'; or 'clandestine intelligence activities' by a foreign network or agent." *Id.* at 59. "Agent of a foreign power" includes any person who "knowingly engages in sabotage or international terrorism" or knowingly participated in "activities that are in preparation therefore." 50 U.S.C. § 1801(b)(2)(C). The use of information obtained through FISA warrants has been held constitutional in prosecutions against spies and terrorists on several occasions. *United States v. Cavanagh*, 807 F.2d 787 (9th Cir. 1987) (finding FISA wiretaps constitutional and properly used in the indictment of a defendant alleged to have attempted to pass classified information to the Soviets); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987) (finding information gained through FISA warrants used to indict former National Security Agency employee with espionage was constitutional); *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984). The defendant was charged with transporting explosives to Ireland from the United States for use against the British Army and argued that evidence gained through FISA surveillance and used against him was unconstitutional. *Duggan*, 743 F.2d at 64. The court dismissed this argument as without merit. *Id.* at 71-76.

143. 50 U.S.C. § 1801-1805; Gaudet, *supra* note 119, at 231.

144. 50 U.S.C. § 1804.

145. *Id.* § 1823 (1994 & Supp. III 1997). Physical searches were not included under FISA until the law was amended in 1994. *Id.*; see Robinson, *supra* note 140, at 64. "The applications must meet detailed and specific criteria. . . . [including] a 'detailed description of the nature of the information sought and of the type of communication or activities to be subject to the surveillance.'" Robinson, *supra* note 140, at 64.

judges who secretly review these applications.¹⁴⁶ However, because the standards for obtaining a FISA wiretap are lower than those for obtaining a criminal wiretap,¹⁴⁷ information gathered by a FISA warrant may not be used in a criminal proceeding, except in limited circumstances.¹⁴⁸ Furthermore, if the target of the FISA surveillance is a "United States Person," certain minimization procedures must be followed to insure that the information sought is necessary to the investigation.¹⁴⁹

In emergency situations, FISA permits the Attorney General to authorize warrantless searches for periods of up to one year, as long as such surveillance is demonstrated, in writing, to be solely directed at communication between or among foreign powers.¹⁵⁰ Specifically,

146. See 50 U.S.C. § 1803(a) (creating the FISA court). The judges are authorized to approve the search as long as they find probable cause to believe that the target of the search is a foreign power or an agent of a foreign power, and that the premises or property to be searched is "owned, used, possessed by or is in transit to or from" an agent of a foreign power or a foreign power. *Id.* § 1824(a)(3). See generally Sanford L. Dow, *Airport Security, Terrorism, and the Fourth Amendment: A Look Back and A Step Forward*, 58 J. AIR L. & COM. 1149, 1194-96 (1993). By enacting FISA, Congress meant to provide guidelines for the executive branch in conducting electronic surveillance for foreign intelligence purposes which would also guarantee protections of individual privacy and other rights. *Id.* at 1194. Furthermore, the FISA court was created to provide oversight to the Executive's power to direct electronic foreign intelligence surveillance. *Id.* In 1979, 199 FISA orders were granted by the FISA court. Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Orders, 1979-1999*, at http://222.308c.94g/privacy/wiretap/stats/fisa_stats.html (last visited Jan. 5, 2002). This number increased to 886 in 1999. *Id.*

147. OCCSSA, 18 U.S.C. §§ 2510-2522, requires the government to meet a strict standard of probable cause, demonstrating that a specific individual is committing a particular crime. Sievert, *supra* note 139, at 1437. FISA, however, only requires probable cause to *believe* that a person is a foreign power or agent of a foreign power—there is no requirement showing probable cause that the person *is* a foreign power or agent of a foreign power. *Id.*; see also 50 U.S.C. § 1801; *supra* Part II.D.2 (discussing OCCSSA requirements).

148. 50 U.S.C. §§ 1806(b), 1825(c). For example, information acquired under FISA may not be disclosed for law enforcement purposes unless it is accompanied by a warning that it may be used in a criminal proceeding. See *id.*; Robinson, *supra* note 140, at 66.

149. See 50 U.S.C. § 1805(h). "Minimization procedures . . . means (1) specific procedures that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of . . . information . . . consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." *Id.* 1801(h)(1). A "United States Person" includes any United States citizen, permanent resident alien, group composed largely of such persons, and United States Corporation. *Id.* § 1801(i).

150. See *id.* § 1802(a)(1)(A)(i)(ii).

Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order . . . to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—

(A) the electronic surveillance is solely directed at—

FISA allows warrantless searches only when no communication involving a United States citizen will be intercepted.¹⁵¹ The Attorney General must submit a certification of the warrantless search to the FISA Court in a sealed envelope, which remains sealed until an application for a warrant is made or the legality of the search is investigated in a court proceeding.¹⁵² Furthermore, warrantless electronic surveillance is allowed only for a twenty-four hour period when the Attorney General certifies that an emergency situation exists requiring immediate surveillance.¹⁵³

In 1998, Congress amended FISA, granting expanded authority for roving wiretaps by easing the requirements.¹⁵⁴ Roving wiretaps are wiretaps that follow an individual from telephone to telephone.¹⁵⁵ Previously, law enforcement had to provide evidence that the target of the surveillance was attempting to thwart interception by purposefully changing telephones.¹⁵⁶ With the 1998 amendment, law enforcement need only demonstrate that the effect of the target's actions is to evade interception.¹⁵⁷ Law enforcement does not have to establish intent on the target's behalf.¹⁵⁸

National security surveillance is only one part of the security measures in place to protect the United States from potential terrorist attacks and acts of sabotage.¹⁵⁹ FISA broadly permits the use of both

(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers . . . or

(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power

Id.

151. *Id.* § 1802(a)(1)(B). The statute requires “no substantial likelihood” that the surveillance will include a U.S. citizen. *Id.*

152. *Id.* § 1802(a)(1). See generally Banks & Bowman, *supra* note 28, at 89-90 (discussing the requirements of FISA when warrantless searches are conducted); Brown & Cinquegrana, *supra* note 33, at 160-61 (discussing FISA and warrantless searches).

153. 50 U.S.C. § 1805(e).

154. See FISA, Pub. L. No. 105-172, 1998 U.S.C.C.A.N. (112 Stat.) 53 (amending 18 U.S.C. § 2518(11)(b) (1994)). “A roving wiretap means that law enforcement agents can listen in on any phone the target might use [just] because he is nearby.” ACLU, *How the USA PATRIOT Act Limits Judicial Oversight of Telephone and Internet Surveillance*, at <http://www.ACLU.org/congress/L102301g.html> (last modified Oct. 23, 2001) [hereinafter *Limits Judicial Oversight*].

155. Banks & Bowman, *supra* note 28, at 111.

156. See 18 U.S.C. § 2518(11).

157. See FISA, Pub. L. No. 105-172.

158. *Id.* This power has been broadened even further by the USA PATRIOT Act of 2001. See *infra* Part III.A-B & Part IV (discussing new standards under the Act and their implications on Fourth Amendment rights).

159. See *infra* Part II.D.4 (discussing the Antiterrorism Act of 1996).

wireless and physical searches for the purpose of gathering foreign intelligence information.¹⁶⁰ However, Congress enacted further measures to protect America, including the enactment of the AEDPA, which expanded the ability to combat both domestic and international terrorism.¹⁶¹

4. The Antiterrorism and Effective Death Penalty Act of 1996

After the 1995 bombing of the Federal Building in Oklahoma City,¹⁶² Congress introduced legislation to expand the federal government's capacity to combat both international and domestic terrorism.¹⁶³ After Congress enacted the AEDPA, President Clinton signed the bill into law on April 24, 1996.¹⁶⁴

The AEDPA primarily provides for stronger immigration laws because it amended the Immigration and Nationality Act.¹⁶⁵ These amendments allow for the use of secret evidence in deportation hearings

160. See Robinson, *supra* note 140, at 64-65.

161. AEDPA, Pub. L. No. 104-132, 110 Stat. 1214 (1996); Banks & Bowman, *supra* note 28, at 107 (discussing the legislative process behind the enactment of the AEDPA).

162. See *Oklahoma City Tragedy: The Bombing*, *supra* note 2.

163. Banks & Bowman, *supra* note 28, at 107. While the Senate introduced a version of the bill in June 1995, the House did not sign off on it until almost one year after the bombing. *Id.*, at 107; see S. REP. NO. 104-735 (1995) (the Senate's version of the bill); AEDPA, Pub. L. No. 104-132, 1996 U.S.C.C.A.N. (110 Stat.) 1214 (1996) (the final version of the bill enacted into law).

164. See AEDPA, Pub. L. No. 104-132, 110 Stat. 1214 (1996). The Clinton Administration considered the prior anti-terrorism laws to be a confusing patchwork of measures, pushing for enhanced surveillance capabilities for terrorism investigations, which were not included in the final version of the bill. Roberta Smith, *America Tries to Come to Terms with Terrorism: The United States Antiterrorism and Effective Death Penalty Act of 1996 v. British Antiterrorism Law and International Response*, 5 CARDOZO J. INT'L & COMP. L. 249 (1997). The Clinton Administration drafted anti-terrorism legislation in February 1995 to "provide clear Federal criminal jurisdiction for any international terrorist attack that might occur in the United States." *Id.* at 261-62; see also Banks & Bowman, *supra* note 28, at 109.

165. 8 U.S.C. §§ 1158, 1251-1259 (2000); Smith, *supra* note 164, at 270-71. The AEDPA provided for "streamlined deportation proceedings, formation of a 'removal court' to expedite deportation of suspected alien terrorists, new habeas restrictions, and the establishment of the Committee to Study Law Enforcement." *Id.* at 270. The law also empowers the Secretary of State to create a list of foreign terrorist organizations. See 8 U.S.C. § 1189(a)(1) (2000). To be designated as such, the Secretary must find that the organization (1) is foreign, (2) engages in terrorist activity, and (3) threatens the security of the United States or United States nationals. *Id.* Under section 1189, national security encompasses the national defense, foreign relations, or economic interests of the United States. See *id.* § 1189(c)(2). The Secretary may base his or her decision upon classified information, which is not subject to disclosure. *Id.* § 1189(a)(3)(B). However, the Secretary must notify Congress of his or her intent seven days before making such a designation. *Id.* § 1189(a)(2)(A). This designation is effective for two years, but it may be renewed at the end of the initial two-year period by undergoing the same process as required at the time of the initial designation. *Id.* § 1189(a)(4)(A)-(B).

against aliens accused of being terrorists,¹⁶⁶ provide for mandatory detention of certain criminal aliens,¹⁶⁷ and allow banks to freeze certain accounts when there is reason to believe the account owners may be agents of a designated foreign terrorist organization.¹⁶⁸ Furthermore, the AEDPA provides relief for victims, including mandatory victim restitution, jurisdiction for lawsuits against terrorist states, and other assistance to victims of terrorism.¹⁶⁹ It also established a removal court to oversee deportation proceedings of suspected alien terrorists.¹⁷⁰

Although the Act does not pose any specific requirements on the government in gathering intelligence for national security purposes, the AEDPA represents the type of reactionary legislation Congress has passed in the wake of significant events in American history.¹⁷¹ Since the enactment of the AEDPA, relatively few significant changes have been made to anti-terrorism legislation, except for the amendment expanding authority for roving wiretaps under FISA in 1998.¹⁷² After the terrorist attacks of September 11, 2001, however, Congress sought to reassure the American people by once again passing new legislation.¹⁷³

E. September 11, 2001

Prior to September 11, 2001, few Americans seriously considered the possibility of a serious terrorist attack by foreign terrorists on American soil.¹⁷⁴ Many Americans may have thought terrorism was something that occurred primarily in the Middle East or Northern Ireland, but not in the United States.¹⁷⁵ Although terrorist acts on United States soil are not new,¹⁷⁶ no event had caused the number of casualties as did the

166. See AEDPA § 504(e)(3)(A).

167. *Id.* § 507.

168. *Id.* § 219(a)(2)(C); see Norman Dorsen, *Civil Liberties, National Security and Human Rights Treaties: A Snapshot in Context*, 3 U.C. DAVIS J. INT'L L. & POL'Y 143, 149-51 (1997) (arguing that the AEDPA violates civil liberties).

169. AEDPA §§ 204-206.

170. *Id.* § 401.

171. See Dorsen, *supra* note 168, at 148-49.

172. See *supra* Part II.D.3-4 (outlining the evolution of anti-terrorism legislation in the United States).

173. See *infra* Part III.A-B (discussing the enactment of the USA PATRIOT Act of 2001).

174. See Madigan, *supra* note 5 (discussing the shock of the events of September 11, 2001).

175. See *supra* Part I (discussing the impact of terrorism globally).

176. Federal Bureau of Investigation, *30 Years of Terrorism: Terrorism in the United States (1999)*, available at <http://www.fbi.gov/publications/terror/terroris.htm> (last modified June 20, 2001) (discussing the number of domestic and international terrorist attacks on U.S. soil between 1980 and 1999) [hereinafter *30 Years of Terrorism*]. Terrorist events within the United States since the 1970s include the bombing of U.S. Senate buildings in 1971, the bombing of the

attacks on September 11, 2001.¹⁷⁷ A 1999 FBI report on terrorism noted that acts of terrorism worldwide have grown less frequent but more destructive and that terrorists are more interested in weapons of mass destruction.¹⁷⁸ While this FBI report focused on chemical, biological and radiological weapons of mass destruction,¹⁷⁹ on September 11th, the responsible parties created a new weapon of mass destruction—the commercial airliner.¹⁸⁰

The attacks on the World Trade Center and the Pentagon on September 11, 2001 are considered to be the most horrific incidents of international terrorism in United States history.¹⁸¹ Terrorists hijacked four commercial airplanes that morning and flew two directly into the towers of the World Trade Center in New York City, resulting in the

Frances Tavern on Wall Street in 1974, the robbery of a Wells-Fargo armored car in 1983, an attack by the Animal Liberation Front (ALF) in 1987, the assassination of Rabbi Meir Kahane, founder of the Jewish Defense League, in New York City in 1990, the bombing of the World Trade Center in 1993, the bombing of the Oklahoma City Federal Building in 1995, the bombing of Centennial Olympic Park in 1996, and the arrest of Ahmed Ressam while he attempted to enter the United States from Canada with explosives in a suspected attempt to bomb the Los Angeles International Airport. *Id.* at 15-24.

177. *30 Years of Terrorism*, *supra* note 176, at 16. Of the 327 recorded incidents of terrorism or suspected terrorism in the United States between 1980 and 1999, over 2,037 persons were injured, but there were only 205 reported deaths. *Id.* In the events of September 11th, approximately 3,225 people were killed. *See* Talbot, *supra* note 6.

178. *30 Years of Terrorism*, *supra* note 176, at 25. These weapons of mass destruction include the use of sarin gas, as seen in a series of attacks on the Tokyo, Japan subway system in 1995. *Id.*

179. *Id.* The report discusses chemical, biological, and radiological terrorism, as well as agroterrorism and cyberterrorism. *Id.* at 38-40. Agroterrorism is "an attack against agriculture, livestock, or other food supplies with a biological, chemical, or radiological weapon." *Id.* at 39. Cyberterrorism includes "physical attacks on critical U.S. infrastructure—such as electric power, telecommunications, banking and finance, gas and oil, and transportation." *Id.*

180. *See* Madigan, *supra* note 5 (relating the events of the terrorist attack of September 11, 2001); Serge Schmemmann, *U.S. Attacked, President Vows to Exact Punishment for 'Evil,'* N.Y. TIMES, Sept. 12, 2001, at A1.

181. *30 Years of Terrorism*, *supra* note 176, at 16. According to a report issued by the FBI, between 1980 and 1999 there were 327 recorded incidents or suspected incidents of terrorism in the United States. *Id.* Two hundred thirty-nine of these incidents were considered domestic terrorism events, while the other eighty-eight were considered events of international terrorism. *Id.* Between 1968 and 1999, over 14,000 international terrorist attacks took place worldwide, resulting in more than 10,000 deaths. *Id.* at 15. Also between 1980 and 1999, U.S. law enforcement prevented eighty-three plots of domestic terrorism and forty-seven plots of international terrorism. *Id.* at 16. However, in 1996, commentators wrote that there was no terrorism crisis in America from 1985 until 1996, noting that there were only two international terrorist incidents in the United States—the 1993 World Trade Center bombing and a trespassing incident at the Iranian mission to the United Nations. Kopel & Olson, *supra* note 97, at 256-57. Until September 11, 2001, the bombing of the Alfred P. Murrah Federal Building in 1995 remained the most horrific incident of domestic terrorism in American history. *Id.*

complete destruction of the towers.¹⁸² A third plane crashed into the Pentagon in Washington, D.C.,¹⁸³ and the fourth crashed into a field in western Pennsylvania.¹⁸⁴

Initial estimates put the death toll at over 6,000 people from the attacks,¹⁸⁵ but as of December 30, 2001, the total number of deaths was estimated at 3,225.¹⁸⁶ Several passengers made telephone calls from the airplanes and reported that the hijackers were armed with knives and box cutters.¹⁸⁷ Immediately after the attacks, all airports in the United States closed, and the military went on the highest state of alert.¹⁸⁸ President George W. Bush, aboard Air Force One at the time of the attacks, made stops in Louisiana and Nebraska before returning to Washington, D.C.¹⁸⁹

Immediately after the terrorist attacks, the American people asked two key questions. First, Americans asked: "How do we retaliate?"¹⁹⁰ Second, people wanted to know: "How do we protect ourselves in the future?"¹⁹¹ President Bush first reassured the American people that every effort was being made to discover the identity of those

182. Schmemann, *supra* note 180. American Airlines Flight 11, a Boeing 767 out of Boston headed for Los Angeles, crashed into the north tower of the World Trade Center at 8:48 a.m. *Id.* United Airlines Flight 93, also headed from Boston to Los Angeles, struck the south tower at 9:06 a.m., eighteen minutes later. *Id.* Both towers collapsed within the next hour. *Id.*

183. *Id.* At 9:40 a.m., American Airlines Flight 77, also headed to Los Angeles from Washington, D.C., crashed into the western part of the Pentagon. *See id.*

184. *Id.* United Airlines Flight 93, flying from Newark to San Francisco, crashed in a Pennsylvania field soon after Flight 77 struck the Pentagon. *Id.* Two hundred and sixty-six airline passengers died in the four planes. *Id.*; *see also* Madigan, *supra* note 5. Officials speculated that Flight 93 was heading for a fourth target in the nation's capital, but due to the heroics of the passengers and its crew, this mission was foiled. *U.S. Strikes Afghanistan*, WASH. POST, Oct. 8, 2001, at C14, *available at* 2001 WL 28363099 ("A fourth [plane] crashed in Pennsylvania, apparently after the passengers fought back against the terrorists.").

185. *See U.S. Strikes Afghanistan*, *supra* note 184.

186. *See* Talbot, *supra* note 6. Two hundred and eighty-eight people were killed at the Pentagon and in Pennsylvania. *Id.* As of December 21, 2001, only 550 bodies at the World Trade Center had been identified. *Id.* While it is believed that more than 12,000 people made it out of the World Trade Center towers, of the 3,225 who died, approximately fifteen percent of those were rescue workers who rushed in to save lives, but were caught when the towers collapsed. *Id.*

187. *See* Madigan, *supra* note 5 (reporting the events of September 11, 2001); Schmemann, *supra* note 180 (reporting the telephone calls made by passengers from the hijacked planes).

188. *See* Madigan, *supra* note 5; Schmemann, *supra* note 180.

189. The White House, the Pentagon, and the Capitol were evacuated, as were most skyscrapers, national monuments, and tourist attractions throughout the country. Madigan, *supra* note 5; Schmemann, *supra* note 180.

190. *See U.S. Strikes Afghanistan*, *supra* note 184 (describing the beginning of United States retaliation for the events of September 11 with the bombing of Afghanistan).

191. *See infra* Part III.A (discussing Congress' answer to this question).

responsible for the attacks.¹⁹² Nine days later, President Bush positively identified the terrorist organization known as al Qaeda and its leader, Osama bin Laden, as the parties responsible for the attacks.¹⁹³ Then, President Bush answered the first question about retaliation by announcing the official beginning of a “war on terrorism” that would end only when “every terrorist group of global reach has been found, stopped, and defeated.”¹⁹⁴ The U.S. targeted bin Laden’s headquarters and those harboring him, and dropped the first bombs on Afghanistan on October 7, 2001.¹⁹⁵ Congress would soon thereafter answer the second question about how we are to protect ourselves.¹⁹⁶

III. DISCUSSION

Throughout history, Congress has enacted legislation in reaction to decisions by the Supreme Court¹⁹⁷ and significant events in American history, such as the 1995 bombing of the Federal Building in Oklahoma

192. George W. Bush, *Statement by the President in His Address to the Nation* (Sept. 11, 2001), at <http://www.whitehouse.gov/news/releases/2001/09/20010911-16.html>.

Today, our fellow citizens, our way of life, our very freedom came under attack in a series of deliberate and deadly terrorist acts . . . I’ve directed the full resources of our intelligence and law enforcement communities to find those responsible and to bring them to justice. We will make no distinction between the terrorists who committed these acts and those who harbor them.

Id.

193. George W. Bush, *Address to a Joint Session of Congress and the American People* (Sept. 20, 2001), at <http://www.whitehouse.gov/news/releases/2001/09/print/20010920-8.html>.

194. *Id.* The President warned that this war on terror would have no definitive end, and that American lives would be lost in combat. *Id.* He further stated: “Our nation has been put on notice: We are not immune from attack. We will take defensive measures against terrorism to protect Americans.” *Id.*

195. *U.S. Strikes Afghanistan*, *supra* note 184 (reporting that the United States started bombing Afghanistan, the Taliban, Osama bin Laden, and al Qaeda in response to the acts of September 11th—Afghanistan was targeted for harboring both the Taliban and bin Laden); *see also* Richard Morin & Claudia Deane, *Public Support is Overwhelming; Poll Finds 94% Favor Bush’s Ordering Strikes on Afghanistan*, WASH. POST, Oct. 8, 2001, at A05, available at 2001 WL 28363135 (citing a Washington Post-ABC News poll finding that ninety-four percent of Americans supported military action against Afghanistan and continued to endorse Bush’s response to the September 11th attacks); Thom Shanker & Steven Lee Myers, *A Nation Challenged, The Pentagon; Deploying Stealthy B-2’s, Military Promises Day and Night Bombing Campaign*, N.Y. TIMES, Oct. 8, 2001, at B4 (reporting on the first U.S. airstrikes of Afghanistan, and citing the Pentagon as stating the campaign would be “weeklong, nearly day-and-night bombing”).

196. *See infra* Part III.A–B (discussing the enactment of the USA PATRIOT Act of 2001).

197. *See supra* Part II.D.2 (discussing the enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, passed in response to *Katz v. United States*, 389 U.S. 347 (1967)); *supra* Part II.D.3 (discussing the enactment of FISA, passed in response to *Keith*, 407 U.S. 297 (1972)).

City.¹⁹⁸ Immediately after September 11, 2001, Congress once again rose to the challenge in an effort to re-secure American freedom through legislation.¹⁹⁹ On October 26, 2001, President George W. Bush signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).²⁰⁰ The USA PATRIOT Act permits a vast array of methods to gather information on individuals within the United States through enhanced intelligence surveillance procedures, limited judicial oversight of telephone and internet surveillance, and the ability of law enforcement to delay notice of search warrants.²⁰¹

A. *Protecting the United States Through Strengthened Legislation*

Immediately following the September 11th terrorist attacks, Congress partially answered the second question, "How do we protect ourselves in the future?" when it sought to strengthen national security legislation.²⁰² In times of war, civil liberties are often curtailed,²⁰³ and

198. See *supra* Part II.D.4 (discussing the enactment of the AEDPA, passed in response to the bombing of the Federal Building in Oklahoma).

199. See USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

200. *Id.* This Act combines the PATRIOT Act introduced by the House of Representatives and the USA Act introduced by the Senate. See *supra* notes 147-48 and accompanying text. President Bush stated,

[t]he changes, effective today, will help counter a threat like no other our nation has ever faced. We've seen the enemy, and the murder of thousands of innocent, unsuspecting people These terrorists must be pursued, they must be defeated, and they must be brought to justice. And that is the purpose of this legislation.

George W. Bush, *Remarks by the President at the Signing of the Patriot Act*, Anti-Terrorism Legislation (Oct. 26, 2001), at <http://www.whitehouse.gov/news/releases/2001/10/print/20011026-5.html>. The purpose of the act is "to deter and punish terrorist acts in the United States and around the world, [and] to enhance law enforcement investigatory tools" USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

201. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001); ACLU, *How the USA PATRIOT Act Puts The CIA Back in the Business of Spying on Americans* (Oct. 23, 2001), at <http://www.aclu.org/Congress/L102301j.htm> [hereinafter *USA PATRIOT Act and the CIA*]. This information may be shared with the Central Intelligence Agency as well as other non-law enforcement officials, even if it pertains to Americans, and without a court order. *USA PATRIOT ACT and the CIA*, *supra*, at 1.

202. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001); see *Antiterrorism Legislation Gains Momentum in Both Chambers; Lawmakers Offer Assorted Stand-Alone Bills*, 78 INTERPRETER RELEASES 1591 (2001).

203. It is only since the 1960s that Congress used its power to set limits on the President's power to make decisions regarding national security. See *supra* Part II (discussing the involvement of Congress in national security issues). See generally Banks & Bowman, *supra* note 28, at 2-31 (providing a description of American history, from the 1700s forward, when freedoms of American citizenship have been disregarded); Norman Dorsen, *supra* note 168, at 143 (noting times in American history, such as the internment of Japanese-Americans during World War II and the McCarthy era, when American civil liberties were set aside); Kristensen,

since the enactment of FISA²⁰⁴ and the AEDPA,²⁰⁵ lawmakers have struggled with the task of protecting the country from terrorism while not exceeding the limits of the Constitution.²⁰⁶ This debate resurfaced when Congress introduced the USA PATRIOT Act, which was designed to strengthen prior legislation and the methods used to insure national security.²⁰⁷

On September 17, 2001, Attorney General John Ashcroft presented Congressional leaders with the Bush administration's proposal to

supra note 126, at 20 (reviewing times in American history, from the Alien and Sedition Acts passed in 1798 through the internment of Japanese-Americans during World War II, McCarthyism, and the Cold War when the civil liberties of American citizens have been set aside due to fear); Col. Thomas W. McShane, *Life, Liberty and the Pursuit of Security—Balancing American Values in Difficult Times*, PA. LA W., Dec. 23, 2001, at 46 (discussing times in America's history when restrictions have been imposed on domestic freedom).

204. See *supra* Part II.D.3 (discussing the 1978 passage of the FISA).

205. See *supra* Part II.D.4 (discussing legislation passed in the wake of the Oklahoma City bombing in 1995).

206. It is of great importance that legislation maximize security without minimizing civil liberties to the point that it violates the Constitution. See Lawrence D. Sloan, *Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 DUKE L.J. 1467, 1467 (2001). Senator Frank Church, who in 1975, after leading a congressional committee that investigated abuses by the National Security Agency and other members of the United States intelligence community, warned that

[the] capability at any time could be turned around on the American people and no American would have any privacy left, such [is] the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. . . . [T]he technological capacity that the intelligence community has given the government could enable it to impose total tyranny. . . . [W]e must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return.

Id.; see also Banks & Bowman, *supra* note 28, at 4.

The Fourth Amendment concern in national security matters arises because the same techniques used in enforcing the criminal laws are used in gathering intelligence. Likewise, some information gathered for intelligence purposes may subsequently be used in criminal prosecutions. Thus, invasions of privacy that are accepted as necessary evils in enforcing the criminal laws may occur when the government seeks intelligence information.

Banks & Bowman, *supra* note 28, at 4; Chiarella & Newton, *supra* note 139, at 25-26 (stating that "[n]o governmental interest is more fundamental than guaranteeing the security of the nation [because] [o]nly in a secure nation can the rights and liberties guaranteed by the Constitution be secure").

207. See Jonathan Krim, *Anti-Terror Push Stirs Fears for Liberties; Rights Groups Unite to Seek Safeguards*, WASH. POST, Sept. 18, 2001, at A17, available at 2001 WL 27733263 (reporting that "[a] coalition of public interest groups from across the political spectrum has formed to try to stop Congress and the Bush administration from rushing to enact counterterrorism measures before considering their effect on Americans' privacy and civil rights"); Robin Toner, *After the Attacks: Civil Liberties; Some Foresee a Sea Change in Attitudes on Freedoms*, N.Y. TIMES, Sept. 15, 2001, at A16, available at 2001 WL 27397567 (quoting Senator Trent Lott stating that, "[w]hen you are at war, civil liberties are treated differently. We cannot let what happened yesterday happen in the future").

enhance and strengthen terrorism legislation.²⁰⁸ The purpose of the legislation, entitled the Mobilization Against Terrorism Act, was to enhance the ability of the government to eliminate terrorist organizations, prevent terrorist attacks, and punish terrorists.²⁰⁹ The key issues of the proposal included intelligence gathering, immigration, criminal justice, and money laundering.²¹⁰ Primarily, the administration meant to broaden the intelligence community's abilities to conduct roving searches of people suspected of terrorism, to detain and deport persons suspected of terrorist involvement, and to remove any statute of limitations on crimes of terrorism.²¹¹ The proposal also expanded the ability of the Department of Justice to place wiretaps on telephones and computer terminals of anyone suspected of terrorism or of having connections to suspected terrorist organizations.²¹² This proposal

208. Mobilization Against Terrorism Act, available at http://www.eff.org/Privacy/Surveillance/20010919_mata_bill_draft.html (Sept. 19, 2001); see John Lancaster & Jonathan Krim, *Ashcroft Presents Anti-Terrorism Plan to Congress; Lawmakers Promise Swift Action, Disagree on Extent of Measures*, WASH. POST, Sept. 20, 2001, at A24, available at 2001 WL 27733536; Philip Shenon & Alison Mitchell, *After the Attacks: Congress; Lawmakers Hear Ashcroft Outline Antiterror Plans*, N.Y. TIMES, Sept. 17, 2001, at A5, available at 2001 WL 27398018.

209. United States Department of Justice, *Attorney General Ashcroft Outlines Mobilization Against Terrorism Act* (Sept. 24, 2001), at <http://www.usdoj.gov/opa/pr/2001/September/492ag.htm> (providing an overview of the administration's proposal). Mr. Ashcroft stated that the purpose of the legislation is to "provide the President and the Department of Justice with the tools and resources necessary to disrupt, weaken, thwart, and eliminate the infrastructure of terrorist organizations, to prevent or thwart terrorist attacks, and to punish perpetrators of terrorist acts." *Id.*

210. Mobilization Against Terrorism Act, *supra* note 208; see Shenon & Mitchell, *supra* note 208; Attorney General John Ashcroft, *Testimony Before the House Committee on the Judiciary* (September 24, 2001), at http://www.usdoj.gov/ag/agcrisisremarks9_24.htm [hereinafter *Ashcroft Testimony*]. Mr. Ashcroft testified that previous law enforcement tools enacted to protect national security were crafted for outdated technology—for rotary telephones, but not email, the Internet, mobile communications and voice mail. *Ashcroft Testimony, supra*. He stated that the administration's proposal would allow for: roving wiretap surveillance, increasing the ability for law enforcement to share information with national security agencies, increasing the ability to prosecute terrorists and those who harbor terrorists, strengthening the ability of the Immigration and Naturalization Service to "detain or remove" suspected alien terrorists, strengthening money laundering laws, and providing "swift emergency relief" to victims of terrorism and their families. *Id.*; see also Attorney General John Ashcroft, *Prepared Remarks, Senate Committee on the Judiciary* (Sept. 25, 2001), at http://www.usdoj.gov/ag/agcrisisremarks9_25.htm.

211. *Ashcroft Testimony, supra* note 210.

212. Philip Shenon, *A Nation Challenged: Congress; Ashcroft Wants quick Action on Broader Wiretapping Plan*, N.Y. TIMES, Sept. 18, 2001, at B4, available at 2001 WL 28004239. The proposed legislation also included "new powers for the Justice Department to fight money laundering, tougher penalties for those who harbor terrorists and removal of the statute of limitations . . . for prosecuting terrorists." *Id.* Several lawmakers stated they wanted quick action regarding any legislative changes, but also wanted to ensure that privacy rights were protected and that time was still allowed to debate the pros and cons of any proposed changes. *Id.*; see also Shenon & Mitchell, *supra* note 208. Senator Patrick J. Leahy of Vermont stated, "[w]e do not

provided the framework for the introduction of the Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001²¹³ introduced by the House of Representatives and the Uniting and Strengthening America (USA) Act of 2001²¹⁴ introduced by the Senate, which eventually became the USA PATRIOT Act of 2001.²¹⁵

After two weeks of debate and compromise, on October 2, 2001 Representative James F. Sensenbrenner, Jr. introduced the PATRIOT Act of 2001 into the House of Representatives, with the primary purpose to deter and punish terrorist acts in the United States and to enhance the ability of law enforcement to investigate potential and actual acts of terrorism.²¹⁶ The Uniting and Strengthening America (USA) Act of 2001 was introduced in the Senate on October 4, 2001.²¹⁷ On October 12th, the Senate approved its version of the bill with a vote of ninety-six to one.²¹⁸ The following day, the House approved its

want the terrorists to win by having basic protections taken away from us," as he cautioned Congress to not rush too quickly to pass legislation. Neil A. Lewis & Philip Shenon, *A Nation Challenged: Safety and Liberty; Senate Democrat Opposes White House's Antiterrorism Plan and Proposes Alternative*, N.Y. TIMES, Sept. 20, 2001, at B6, available at 2001 WL 28004806.

213. See *infra* note 216 and accompanying text (discussing the House of Representative bill).

214. See *supra* notes 208-12 and accompanying text (discussing the Senate bill).

215. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

216. H.R. 2975, *Bill Summary & Status for the 107th Congress*, at <http://thomas.loc.gov> (last modified Jan. 23, 2002). The bill was introduced by Rep. James F. Sensenbrenner, Jr. *Id.*; see Neil A. Lewis & Robert Pear, *A Nation Challenged: Congress; Negotiators Back Scaled-Down Bill to Battle Terror*, N.Y. TIMES, Oct. 2, 2001, at A1, available at 2001 WL 28008671 (reporting that House Democrats and Republicans reached an agreement on a bill giving law enforcement officials authority to wiretap suspected terrorists, share intelligence information, and monitor Internet communications).

The compromised bill resulted after complaints from both Democrats and Republicans that the Bush Administration's Mobilization Against Terrorism Act proposal overly expanded the government's powers at the expense of civil liberties. Lewis & Pear, *supra*. One key change from the administration's bill was the implementation of a two-year sunset provision on the expanded wiretap powers. *Id.* The House bill also eliminated provisions in the administration bill that required schools to disclose certain information about foreign students to any government agency requesting it by stating they had a "reasonable need" to obtain it. *Id.*; see also H.R. 2975.

217. USA Act of 2001; S. 1510, *Bill Summary & Status for the 107th Congress*, at <http://thomas.loc.gov> (last modified Jan. 23, 2002). The bill was introduced by Sen. Thomas A. Daschle. *Id.* The Senate version of the bill had no sunset requirement for the wiretap provisions. *Id.*; see Neil Lewis & Robert Pear, *A Nation Challenged: Legislation; Terror Laws Near Votes in House and Senate*, N.Y. TIMES, Oct. 5, 2001, at B8, available at 2001 WL 29156353.

218. USA Act of 2001, S. 1510, *Bill Summary & Status for the 107th Congress*, at <http://thomas.loc.gov> (last modified Jan. 23, 2002). Senator Russell Feingold of Wisconsin was the lone dissenter in the senate. John Lancaster, *Senate Passes Expansion of Electronic Surveillance; Anti-Terrorism Bill is Set for House Debate Today*, WASH. POST, Oct. 12, 2001, at A01, available at 2001 WL 29161259. Senator Feingold stated:

"There have been periods in our nation's history when civil liberties have taken a back seat to what appeared at the time to be the legitimate exigencies of war . . . [including] the Alien and Sedition acts, the suspension of habeas corpus during the Civil War, the

version of the anti-terrorism bill with a vote of three hundred thirty-seven to seventy-nine.²¹⁹

The passage of both bills gave law enforcement the increased power they had sought for many years, but which was previously rejected by Congress as “overly intrusive and possibly unconstitutional.”²²⁰ Both bills authorized roving wiretaps in intelligence investigations, made it easier for investigators to track phone, e-mail, and Internet traffic, and permitted prosecutors to share grand jury and wiretap transcripts with intelligence agencies.²²¹ Unlike the administration’s proposal, both the House and Senate bills included a provision allowing secret searches of a suspect’s property.²²²

B. The USA PATRIOT Act

On October 25, 2001, Congress passed the USA PATRIOT Act of 2001, which was then signed into law by President Bush on October 26th.²²³ The Senate debated the final version of this bill for one day,

internment of Japanese Americans, German Americans, and Italian Americans during World War II, the blacklisting of supposed communist sympathizers during the McCarthy era, and the surveillance and harassment of antiwar protesters, including Dr. Martin Luther King Jr.”

Jonathan Krim & Robert O’Harrow Jr., *Bush Signs Into Law New Enforcement Era; U.S. Gets Broad Economic Powers*, WASH. POST, Oct. 27, 2001, at A06, available at 2001 WL 29165152.

219. H.R. 2975, *Bill Summary & Status for the 107th Congress*, at <http://thomas.loc.gov> (last modified Jan. 23, 2002).

220. See John Lancaster, *Anti-Terrorism Bill is Approved; Bush Cheers House’s Quick Action, but Civil Liberties Advocates are Alarmed*, WASH. POST, Oct. 13, 2001, at A01, available at 2001 WL 29161530; Jill Zuckman, *Bill Ok’d to Expand Anti-terror Powers*, CHI. TRIB., Oct. 13, 2001, § 1, at 1, available at 2001 WL 4125171.

221. See H.R. 2975; S. 1510; Lancaster, *supra* note 220.

222. See H.R. 2975; S. 1510; Zuckman, *supra* note 220.

223. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). There are ten separate provisions to the Act:

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; and

Title X, Miscellaneous.

Id. This section will focus primarily upon Titles II, III, and IX. The Senate passed the legislation on October 25, 2001, and it passed in the House on October 24, 2001. See Sonia Arrison, *Attack*

passing the legislation just six weeks after the September 11th terrorist attacks.²²⁴ The USA PATRIOT Act provides for enhanced intelligence surveillance procedures,²²⁵ limited judicial oversight of telephone and Internet surveillance,²²⁶ and the ability of law enforcement to delay notice of search warrants.²²⁷

1. Enhanced Intelligence Surveillance Procedures

Title II of the USA PATRIOT Act, entitled Enhanced Surveillance Procedures, amends the FISA²²⁸ and the federal criminal code²²⁹ to authorize the interception of wire, oral, and electronic communications for the production of evidence of specified chemical weapons, terrorism offenses, and computer fraud and abuse.²³⁰ Title II of the USA PATRIOT Act also amends Rule Six of the Federal Rules of Criminal Procedure to permit law enforcement agents to provide the CIA with foreign intelligence and counter-intelligence information revealed to grand juries without a court order.²³¹

On America—New Anti-Terrorism Law Goes Too Far, SAN DIEGO UNION-TRIB., Oct. 31, 2001, at B9, available at 2001 WL 27297744; Adam Clymer, *Antiterrorism Bill Passes; U.S. Gets Expanded Powers*, N.Y. TIMES, Oct. 26, 2001, available at 2001 WL 29615593; Susan Milligan, *Vote Expands Authorities' Clout in Hunt For Terrorists—Senate Votes to Ease Limits on Agencies' Terror Probe*, BOSTON GLOBE, Oct. 26, 2001, at A1, available at 2001 WL 3958684.

224. Compare the almost immediate and reactionary enactment of the USA PATRIOT Act with the enactment of the AEDPA, which was not enacted until one year after the Oklahoma City Bombing. See *supra* Part II.C.4 (discussing the enactment of the AEDPA).

225. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); see *infra* notes 226-44 and accompanying text (discussing the enhancement of surveillance procedures).

226. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); see *infra* notes 240-52 and accompanying text (discussing limited judicial review of telephone and internet surveillance).

227. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001); see *infra* notes 257-63 and accompanying text (discussing delayed notice of search warrants); see also *USA PATRIOT Act and the CIA*, *supra* note 201. This information may be shared with the Central Intelligence Agency as well as other non-law enforcement officials, even if it pertains to Americans, and without a court order. *USA PATRIOT Act and the CIA*, *supra* note 201.

228. FISA, 50 U.S.C. §§ 1801-1863 (2000).

229. FED. R. CRIM. P. 6 (2000).

230. USA PATRIOT Act §§ 201-225. Senator Leahy stated,

"[t]his bill will authorize the expanded sharing with intelligence agencies of information collected as part of a criminal investigation, and the expanded use of foreign intelligence surveillance tools and information in criminal investigations . . . enter[ing] new and uncharted territory by breaking down traditional barriers between law enforcement and foreign intelligence."

147 CONG. REC. S10990, S10992 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy). Senator Orrin Hatch stated that, "[t]hese provisions sharpen the tools used by the FBI, CIA, and NSA for collecting intelligence on international terrorists and other targets under FISA, 50 U.S.C. §§ 1801-63." 147 CONG. REC. S10990, S11055 (daily ed. Oct. 25, 2001) (statement of Sen. Hatch).

231. USA PATRIOT Act § 203(a). Foreign intelligence information is

Furthermore, Title II allows law enforcement officers to share electronic, wire, and oral interception information with the CIA, amending 18 U.S.C. § 2517.²³² Specifically, this section allows any investigative or law enforcement officer or government attorney to disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence.²³³

The USA PATRIOT Act also expands the ability of the CIA and other governmental agencies to gather information about Americans by allowing law enforcement and intelligence-gathering agencies to disclose any information related to foreign intelligence or counterintelligence²³⁴ obtained as part of a domestic criminal

information, whether or not concerning a United States person, that relates to the ability of the United States to protect against (aa) actual or potential attack . . . (bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (cc) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of [a] foreign power; or (II) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to (aa) the national defense or the security of the United States; or (bb) the conduct of foreign affairs of the United States.

Id.

Senator Leahy explained that, “[t]he law is changed not only to permit the wider sharing of information from grand juries, domestic law enforcement wiretaps, and criminal investigations generally . . . but also to require Federal law enforcement agencies to share this information with intelligence agencies through the Director of Central Intelligence.” 147 CONG. REC. S10990, S10992 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy). Even if the information is about “entirely lawful activities, business transactions, political relationships, or personal opinions,” it potentially may be shared whenever a criminal investigation “acquires information about an American citizen’s relationship with a foreign country or its government.” *Id.*

232. USA PATRIOT Act § 203(b). Electronic, wire, and oral interception information includes the intercepts of telephone and Internet conversations, providing for no meaningful restrictions on subsequent use of the recorded conversations. *Id.* Furthermore, it does not prohibit the CIA from sharing information gained through foreign intelligence surveillance for use in a criminal investigation. *Id.*

233. USA PATRIOT Act § 203(b)(1). The section provides that the Attorney General establish procedures regarding how to disclose this information. *Id.* § 203(c); *see supra* note 231 (defining foreign intelligence information).

234. USA PATRIOT Act § 203(d)(1). For this section, foreign intelligence or counterintelligence information is defined in section 3 of the National Security Act of 1947, 50 U.S.C. § 401(a). “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. § 401(a)(2). “Counterintelligence information” is defined as “information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.” *Id.* § 401(a)(3); *see supra* note 231 (defining foreign intelligence information).

investigation.²³⁵ Under this section, a court order is not required prior to the sharing of this information, and the definition of “foreign intelligence information” is broadened.²³⁶ The USA PATRIOT Act also mandates the expeditious disclosure to the Director of the CIA of foreign intelligence information with respect to criminal investigations, obtained by the Department of Justice or any element of that department.²³⁷ Once again, the law empowers the Attorney General to develop guidelines for this type of disclosure.²³⁸

The USA PATRIOT Act expands the role of the Director of the CIA,²³⁹ specifying that the Director work closely with the Attorney General to establish requirements and priorities for gathering any foreign intelligence information under FISA.²⁴⁰ The USA PATRIOT Act does not allow the CIA Director to direct or manage electronic surveillance or physical search operations,²⁴¹ and the CIA’s charter specifically bars it from engaging in internal security functions.²⁴² The USA PATRIOT Act, however, amends that charter by allowing the Director of the CIA to be intimately involved in domestic security, somewhat negating the restriction placed by the CIA charter.²⁴³ As the role of the Director of the CIA is expanded in national security surveillance, the role of the judiciary in overseeing certain searches and seizures is diminished.²⁴⁴

235. USA PATRIOT Act § 203(d)(1).

236. *See supra* note 231 (defining foreign intelligence information); *see also supra* note 140 (laying out the previous definition of foreign intelligence information).

237. USA PATRIOT Act, § 905(a). This section amends Title I of the National Security Act of 1947, 50 U.S.C. § 402 (i)(1)–(2).

238. USA PATRIOT Act § 905(a)(2)–(a)(c). “In section 905, where the bill requires disclosure to intelligence agencies from criminal investigations, the Attorney General is authorized to make exceptions and must issue implementing procedures [that] will be closely examined by the Senate Judiciary Committee.” 147 CONG. REC. S10990, S10992 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

239. USA PATRIOT Act § 901 (amending section 103(c) of the National Security Act of 1947, 50 U.S.C. 403-3(c)). FISA, 50 U.S.C. § 1801.

240. USA PATRIOT Act § 901.

241. *Id.*

242. 50 U.S.C. § 403-3(d)(1). “In the Director’s capacity as head of the Central Intelligence Agency, the Director shall: . . . collect intelligence through human sources and by other appropriate means, except that the Agency shall have no police, subpoena, or law enforcement powers or internal security functions.” *Id.*

243. USA PATRIOT Act § 901. The Director of the CIA shall “provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act [FISA] is disseminated so it may be used efficiently and effectively for foreign intelligence purposes.” *Id.*

244. *See* USA PATRIOT Act §§ 216, 206, 218; *infra* Part III.B.2 (discussing the shrinking role of the judiciary under the Act).

2. *Judicial Oversight of Telephone and Internet Surveillance*

The USA PATRIOT Act limits judicial oversight of telephone and Internet surveillance²⁴⁵ and allows voice mail messages to be seized on the authority of a probable cause search warrant.²⁴⁶ The USA PATRIOT Act amends 18 U.S.C. § 3121(c) by requiring a trap and trace device²⁴⁷ and restricting recoding or decoding so as not to include the contents of a wire or electronic communication.²⁴⁸ 18 U.S.C. § 3121(a) was amended, requiring the FISA court to grant a court order for a pen register²⁴⁹ or trap and trace device anywhere within the United States as long as the government certifies the information may be relevant to an ongoing criminal investigation.²⁵⁰ Any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate execution of the order is required to comply with the order.²⁵¹ Section 3121(a) was further amended, requiring that specified records be kept on any pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service open to the public.²⁵²

Previously under FISA, a law enforcement officer could obtain an order requiring a telephone company to reveal the numbers dialed to and from a particular telephone only by certifying that the information

245. USA PATRIOT Act §§ 216, 206, 218.

246. *Id.* § 209. Section 209 amends 18 U.S.C. §§ 2510, 2703. *Id.*; *supra* Part II.A (discussing the Fourth Amendment). Previously, sections 2510 and 2703 only included electronic, but not wire, communications. *See* 18 U.S.C. §§ 2510, 2703 (2000).

247. A “trap and trace device” is “a device or process which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.” 18 U.S.C. § 3127(4) (1994).

248. USA PATRIOT Act § 216(a)(1)–(3). “The bill would modify the pen register and trap and trace statutes to allow for nationwide service of a single order for installation of these devices, without the necessity of returning to court for each new carrier.” 147 CONG. REC. S10990, S10999 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy). While previously every time a surveillance target switched telephone lines the Government was required to obtain a new court order for the new line, this bill allows the court order to follow the person, negating the need to obtain a new order. *Id.*

249. A pen register is a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached. 18 U.S.C. § 3127(3) (1994). A similar definition states, “[a] mechanical device that logs dialed telephone numbers by monitoring electrical impulses.” BLACK’S LAW DICTIONARY 926 (7th ed. abridged 1996).

250. 18 U.S.C. § 3121(a) (1994).

251. *Id.*

252. *Id.*

to be obtained is relevant to an ongoing criminal investigation.²⁵³ The USA PATRIOT Act, however, extends the ability of law enforcement to access Internet communications, including dialing, routing, and signaling information.²⁵⁴ The USA PATRIOT Act also permits a judge or magistrate to issue a warrant without naming the place or person to be searched anywhere within the United States, thereby enabling the law enforcement agent to insert the name of the person or place.²⁵⁵ Usually, a judge with jurisdiction over the place to be searched authorizes the specific search and the area to be searched, thus helping to prevent abuses such as an accidental search of the wrong home.²⁵⁶

Furthermore, the USA PATRIOT Act allows the government to obtain roving wiretaps, or wiretaps that follow an individual from telephone to telephone, whenever the actions of the wiretapping target might thwart the identification of a specified person.²⁵⁷ The USA PATRIOT Act also extends the duration of FISA surveillance²⁵⁸ of non-United States citizens who are agents of a foreign power to the duration specified in the application or a period of 120 days, whichever is less.²⁵⁹ Previously, FISA required law enforcement to demonstrate that the "sole or main purpose" of the surveillance was to gather foreign intelligence information before obtaining an application for an electronic surveillance order or search warrant.²⁶⁰ The USA PATRIOT Act amends the "sole or main purpose" language, broadening the purpose to "a significant purpose" and lessening the burden of proof the government must demonstrate in order to obtain a FISA warrant.²⁶¹

253. 18 U.S.C. § 3122(b)(2) (2000). "An application under subsection (a) of this section shall include—(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." *Id.*

254. USA PATRIOT Act § 216(a).

255. 18 U.S.C. § 3123(a)(1) (1994).

256. This judicial authority also ensures that law enforcement does not conduct surveillance on persons not intended to be investigated by that particular warrant. *See Limits Judicial Oversight, supra* note 154.

257. USA PATRIOT Act § 206. The changes to § 206 bring FISA into line with criminal procedures that allow surveillance to follow a person, rather than requiring a separate court order identifying each telephone company or other communication common carrier whose assistance is needed. . . . [This section] recognizes the ease with which targets of investigations can evade surveillance by changing phones. 147 CONG. REC. S10998 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

258. FISA authorizes surveillance for foreign intelligence gathering purposes. *See supra* notes 139-61 and accompanying text (discussing the purpose of FISA).

259. USA PATRIOT Act § 207.

260. 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B).

261. USA PATRIOT Act § 218.

3. Delayed Notice of Search Warrants

Finally, the USA PATRIOT Act authorizes federal district courts to delay required notices of the execution of a warrant if immediate notice might have an adverse result or under other specified circumstances.²⁶² The court has the authority to delay notice when it finds reasonable cause to delay the warrant, such as the possibility that execution of the warrant will have an adverse result,²⁶³ when the warrant prohibits the seizure of any tangible property or wire or electronic communication,²⁶⁴ or when the warrant provides that notice should be given within a specified period of time and that time is extended by the court for good cause shown.²⁶⁵ The statute does not, however, define reasonable cause or reasonable necessity.²⁶⁶ Furthermore, while FISA previously only authorized delayed notice for searches of oral and wire communications²⁶⁷ this amendment would also permit delayed notice of searches for physical evidence.²⁶⁸

IV. ANALYSIS

Effective, comprehensive anti-terrorism legislation is required in order to protect the national security of the United States.²⁶⁹ Congress,

262. *Id.* § 213. This section amends 18 U.S.C. § 3103a. *Id.* The Second and Ninth Circuits have recognized a limited exception to the requirement that even if a search occurs when the owner of the premises is not present, the owner must receive notice that the premises has been lawfully searched pursuant to a warrant. *United States v. Villegas*, 899 F.2d 1324 (2d Cir. 1990); *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986); *supra* Part II.B (discussing the Fourth Amendment requirements for search and seizure). The Second and Ninth Circuits have held that when specifically authorized by the issuing judge or magistrate, notice of a search may be delayed in order to avoid compromising an ongoing investigation or for some other good reason. *Villegas*, 899 F.2d at 1336-38; *Freitas*, 800 F.2d at 1457. Both cases dealt only with situations in which a physical search occurred, but no tangible property was removed. *Villegas*, 899 F.2d at 1324; *Freitas*, 800 F.2d at 1451. The Second Circuit explained that these searches were “less intrusive than a conventional search with physical seizure because the latter deprives the owner not only of privacy but also for the use of his property.” *Villegas*, 899 F.2d at 1337. The Ninth Circuit held that, while notice of the search could be delayed, it must be provided within a reasonable period thereafter, generally no more than seven days. *Freitas*, 800 F.2d at 1456.

263. *See* USA PATRIOT Act § 213(2).

264. *See id.*

265. *See id.* Senator Hatch testified that the so-called “sneak and peek” search warrants are already used throughout the United States, stating that “[t]he bill simply codifies and clarifies the practice making certain that only a Federal court, not an agent or prosecutor, can authorize such a warrant.” 147 CONG. REC. S10990, S11023 (daily ed. Oct. 25, 2001) (statement of Sen. Hatch).

266. *See* USA PATRIOT Act § 213.

267. *See* ACLU, *How the USA Patriot Act Expands Law Enforcement “Sneak and Peek” Warrants* (Oct. 23, 2001), at <http://www.aclu.org/congress/L102301b.html> [hereinafter *Expands Sneak and Peek Warrants*].

268. *See* USA PATRIOT Act § 213.

269. *See supra* Part II.C–E (discussing the reasons for national security legislation).

however, overreached its power by expanding the role of the Director of the CIA in domestic intelligence gathering,²⁷⁰ broadening the surveillance powers of the intelligence community while limiting judicial oversight,²⁷¹ and delaying the notice requirement for search warrants.²⁷² Though it is important to protect the United States from the horrors of terrorism, there must be a balance between safety and privacy.²⁷³ Ultimately, the USA PATRIOT Act sets aside the all too important protections guaranteed by the Fourth Amendment in the name of fighting terrorism.²⁷⁴

A. *The USA PATRIOT Act Violates Fourth Amendment Protections*

The wiretapping and intelligence provisions in the USA PATRIOT Act improperly minimize the role of judges in ensuring that law enforcement wiretapping is conducted legally and permits intelligence authorities to bypass procedures that protect people's privacy.²⁷⁵ Because FISA searches are always secret, the target of FISA surveillance does not know when a search occurs and cannot obtain

270. See *supra* Part III.B.1 (discussing enhanced surveillance procedures, information sharing abilities, and the increased role of the Director of the CIA).

271. See *supra* Part III.B.2 (discussing the expansion of telephone and internet surveillance).

272. See *supra* Part III.B.3 (discussing delayed notice requirements for search warrants). Some of the provisions of the Act sunset in four years; however, the sections discussed in this comment do not have sunset provisions. 147 CONG. REC. S10990, S10991 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy). A sunset law is a "statute under which a governmental agency or program automatically terminates at the end of a fixed period unless it is formally renewed." BLACK'S LAW DICTIONARY 1167 (7th ed. abridged 1996).

273. See Testimony of Timothy H. Edgar, ACLU Legislative Counsel (Oct. 12, 2001), at <http://www.aclu.org/congress/L101201b.html> (testifying that any anti-terrorism legislation "must provide the maximum effectiveness in the fight against terrorism while minimizing any adverse impact on civil rights and civil liberties"); ACLU, *Letter to Senate Urging it to Vote No on Final Version of the USA PATRIOT Act* (Oct. 23, 2001), at <http://www.aclu.org/congress/L102301k.html> (stating that "[w]e can be safe and fight terrorism without substantially surrendering our civil liberties, and without giving enormous, unwarranted power to the executive branch—which can be used against U.S. citizens—unchecked by meaningful judicial review"); see also *Anti-Terror Bill*, LAS VEGAS REV. J., Oct. 25, 2001, available at 2001 WL 9542036 (discussing the possibility that the Act's provisions would grant new powers to the government to spy on law-abiding citizens as well as suspected terrorists); Arrison, *supra* note 223; Krim & O'Harrow, *supra* note 218 (reporting that the new law gives government "a freer hand to conduct searches . . . eavesdrop on Internet communication . . . reduc[ing] the need for subpoenas, court orders or other legal checks to enable law enforcement to move more quickly").

274. See *supra* Part II.A (discussing the requirements set forth by the Fourth Amendment).

275. See *supra* Part III.B.1–2 (discussing the wiretapping and intelligence provisions of the Act); see also ACLU *Legislative Analysis*, *supra* note 11; EPIC, *Analysis of Provisions of the Proposed Anti-Terrorism Act of 2001 Affecting the Privacy of Communications and Personal Information* (Sept. 24, 2001), at http://www.epic.org/privacy/terrorism/ata_analysis.html [hereinafter *EPIC Analysis*].

discovery of the FISA court order application.²⁷⁶ Therefore, in a criminal prosecution, if the state uses evidence gathered through a FISA search, the target of the search does not have notice of the search, violating the Fourth Amendment.²⁷⁷ The USA PATRIOT Act expands the ability of law enforcement to obtain FISA warrants, voiding early protections worked into FISA by Congress.²⁷⁸

1. New Federal Surveillance Powers are Too Broad

The new federal surveillance powers are too broad, potentially interfering with the everyday lives of innocent United States citizens who show interest in what may be considered unorthodox political beliefs.²⁷⁹ Title II of the USA PATRIOT Act amends FISA, allowing government surveillance of aliens and United States citizens for criminal investigations, when foreign intelligence gathering is a “significant” purpose of the surveillance.²⁸⁰ This amendment allows the FBI to conduct a physical search or to wiretap primarily to obtain evidence of a crime without proving probable cause, violating the Fourth Amendment.²⁸¹ The only reason the FBI needs to obtain a FISA

276. FISA, 50 U.S.C. §§ 1801–1863 (1994 & Supp. 1998); ACLU, *How the USA-PATRIOT Act Enables Law Enforcement to Use Intelligence Authorities to Circumvent the Privacy Protections Afforded in Criminal Cases* (Oct. 23, 2001), at <http://www.aclu.org/congress/L102301i.html> [hereinafter *Enables Law Enforcement*].

277. The Fourth Amendment generally requires the government to obtain a warrant and give notice to the person whose property will be searched, announcing his presence before serving a search warrant. *Wilson v. Arkansas*, 514 U.S. 927, 934 (1995). Absent exigent circumstances, the common law principle of announcement is an element of the reasonableness inquiry under the Fourth Amendment; therefore, a failure to provide notice prohibits the target of the search from verifying the accuracy of the warrant, placing the target at risk for an unreasonable and unconstitutional search. *Id.*

278. See *supra* notes 138-61 and accompanying text (discussing Fourth Amendment protections set forth in FISA).

279. See *Enables Law Enforcement*, *supra* note 276.

280. See *supra* note 261 and accompanying text (discussing how the USA PATRIOT Act broadens FISA); see also ACLU *Legislative Analysis*, *supra* note 11; EPIC *Analysis*, *supra* note 275.

281. Previously under FISA, surveillance was allowed only when foreign intelligence gathering was the “primary” purpose of the investigation. See *supra* notes 259-60 and accompanying text; see *supra* Part II.D.3 (discussing FISA and criminal investigations); *supra* note 29 and accompanying text (describing the probable cause requirement and the Fourth Amendment). See generally ACLU *Legislative Analysis*, *supra* note 11; EPIC *Analysis*, *supra* note 275. “[The Act] allows law enforcement agencies to wiretap and monitor Internet use whenever intelligence gathering constitutes a ‘significant purpose’ of the surveillance. We should not expose American citizens to invasions of privacy under vague phrases such as ‘significant purpose.’” 147 CONG. REC. E1896 (daily ed. Oct. 16, 2001) (statement of Hon. Patsy T. Mink); Kate Martin, *Memorandum to Interested Persons, Federal Law Enforcement and Intelligence Provisions in Proposed Anti-Terrorism Bill* (Oct. 1, 2001), at <http://www.cdt.org/security/01100/cnss.pdf>, at *3 (discussing concerns regarding proposed amendments to FISA).

surveillance warrant is if it is gathering domestic or foreign intelligence information.²⁸² Furthermore, the amendment puts Americans who may share in the religious or political beliefs of the terrorists, or at least have an interest in exploring those ideas, at risk for being placed on a watch list, even if they are completely innocent of any terrorist activity themselves.²⁸³

In criminal investigations, the Fourth Amendment requires that law enforcement officials have probable cause to believe that a crime has been or is being committed in order to conduct a search.²⁸⁴ FISA searches, however, do not require a showing of probable cause of a crime.²⁸⁵ Thus when FISA was enacted, Congress required that the primary purpose of the search or wiretap be to gather foreign intelligence and not to gather information for a criminal investigation.²⁸⁶

Strict application of Fourth Amendment requirements in criminal cases has been applied for good reason: to protect citizens from unauthorized and unreasonable government intrusion.²⁸⁷ The expansion

deleting the primary purpose language and changing it to significant purpose, thus eliminating some of the safeguards in FISA).

282. See Martin, *supra* note 281, at 4-5; *Enables Law Enforcement*, *supra* note 276.

Americans . . . who are believed to have ties to foreign powers could find their homes broken into and their telephones tapped. Though the government would be searching primarily for evidence of crime, the FBI would secretly conduct these searches and record these conversations without showing probable cause of crime to a judge.

Enables Law Enforcement, *supra* note 276; see also Morton H. Halperin & Kate Martin, *Statement Before the Permanent Select Committee on Intelligence of the United States Senate on Legislative Proposals in the Wake of the September 11, 2001 Attacks* (Sept. 24, 2001), at <http://www.cfr.org/public/resource.cgi?pub!4061>.

It is not an anomaly that the government has to go back to court more often [under FISA] than under [OCCSSA] to get authority to continue surveillance of a private person lawfully resident [sic] in the United States. Since the person will never be told of the surveillance nor have an opportunity to move to have the surveillance records purged, it is important that a judge check regularly . . . to be sure that the government's suspicion that the person was acting as the agent of a foreign power was correct

Id.

283. This issue borders on First Amendment freedom of speech, religion, and association concerns, which are beyond the scope of this article. See generally *USA PATRIOT Act and the CIA*, *supra* note 201; Halperin & Martin, *supra* note 282 (discussing First Amendment concerns).

284. See *supra* Part II.A.2 (discussing the Fourth Amendment and the probable cause requirement). In most situations, without probable cause, a search is illegal, ensuring that wiretaps and search warrants are applied only to those involved in criminal activity, not to innocent citizens. See *supra* Part II.D.3; see also *Enables Law Enforcement*, *supra* note 276.

285. See *supra* note 146 and accompanying text (discussing congressional requirements that there be probate laws focusing the target of the investigation to be a foreign power or agent of a foreign power as opposed to the OCCSSA requirement showing probable cause of a crime).

286. *Id.* "If the primary purpose of surveillance is a criminal investigation, the FBI must have probable cause of crime." *Enables Law Enforcement*, *supra* note 276.

287. See *supra* Part II.A (discussing the reasoning behind the Fourth Amendment).

of surveillance powers under OCCSSA and FISA,²⁸⁸ and the expansion of the role of the Director of the CIA, opens the door to abuses by government intelligence agencies. OCCSSA and FISA were designed to protect Americans from these abuses,²⁸⁹ but the USA PATRIOT Act eliminates many of these protections.²⁹⁰

2. The USA PATRIOT Act Ignores the Probable Cause Requirement of the Fourth Amendment When Obtaining a Court Order

Probable cause is no longer required to be shown when obtaining a court order under the USA PATRIOT Act.²⁹¹ This is too great of an invasion into the privacy of innocent individuals and into the areas of the lives of targeted individuals that are of no relevance to the government's investigation.²⁹² Previously, under FISA, law enforcement was able to obtain a pen register or trap and trace order requiring a telephone company to reveal the numbers dialed to and from a particular telephone.²⁹³ Revealing the numbers dialed does not reveal the content of any conversation occurring at those telephone numbers.²⁹⁴ Because very little is revealed, the standard of proof required for this type of warrant is very low: "relevant to an ongoing criminal investigation."²⁹⁵

The USA PATRIOT Act expands the definition of pen register and trap and trace devices to encompass communications from the Internet, including electronic mail and Web surfing.²⁹⁶ The problem, however, is that these types of communication contain data that is far more revealing than telephone numbers.²⁹⁷ Law enforcement can determine which websites a person visits and view subject lines of e-mail

288. See *supra* Part III.B.1 (discussing the expansion of surveillance powers under FISA).

289. See *supra* Part II.D.1 (discussing the past history of abuses by intelligence agencies); see also *Enables Law Enforcement*, *supra* note 276.

290. See *Enables Law Enforcement*, *supra* note 276.

291. *Id.*

292. *Id.*

293. See *supra* Part III.B.2 (discussing pen register and trap and trace devices).

294. See *Limits Judicial Oversight*, *supra* note 154.

295. *Id.* This burden of proof is far less than the probable cause standard usually required in a criminal investigation—the difference is that revealing telephone numbers does not reveal content. *Id.* The revelation of content usually requires evidence of probable cause. *Id.*; see *EPIC Analysis*, *supra* note 275.

296. See *supra* Part III.B.2 (discussing pen register and trap and trace devices); *Enables Law Enforcement*, *supra* note 276; Halperin & Martin, *supra* note 282.

297. *ACLU Legislative Analysis*, *supra* note 11 (providing an overview of potential problems resulting from the expanded definitions of pen register and trap and trace devices); *ACLU, Enables Law Enforcement*, *supra* note 276 (discussing concerns regarding expanding surveillance to email communications).

communications, which is the equivalent of obtaining content, while only having to demonstrate the low standard of proof of “relevant to an ongoing criminal investigation.”²⁹⁸ Therefore, probable cause, usually required for obtaining content, is ignored.²⁹⁹ When surveillance reveals content, the FBI gains significant access to the communications of non-targets and to information that it is not permitted to access under the purported court order.³⁰⁰

3. The Equivalent of Blank Warrants are Permitted

The USA PATRIOT Act permits the equivalent of blank warrants, thus removing the judge’s ability to effectively monitor compliance with the court order.³⁰¹ Without specifying the person or place to be searched, the judge is unable to truly verify that the law enforcement officer or intelligence agency is conducting a search on the correct target and for legitimate reasons, which were part of the protections that the OCCSSA and FISA were implemented to provide.³⁰²

The Fourth Amendment requires that when a court issues a warrant, the person or place to be searched must be specified.³⁰³ If information gained from one particular search suggests that a second place should be searched, law enforcement must go to the judge in that jurisdiction and obtain a warrant specifying the new location.³⁰⁴ Section 216 of the USA PATRIOT Act, however, allows for “nationwide service” of pen register and trap and trace orders, authorizing the equivalent of a blank

298. *ACLU Legislative Analysis*, *supra* note 11. This provision is equivalent “to requir[ing] the librarian to report on the books [a person] had perused while visiting the public library.” *Id.*; *see also Limits Judicial Oversight*, *supra* note 154. Section 216 specifies that content is not to be included in any communications obtained through pen register and trap and trace device surveillance. USA PATRIOT Act § 216 (2001). However, no guidelines are provided to ensure that this type of information is not collected—the FBI will have to separate the addressing information from the content, and retain only the addressing information. *Limits Judicial Oversight*, *supra* note 154.

299. *Limits Judicial Oversight*, *supra* note 154; *see EPIC Analysis*, *supra* note 275.

300. Because the standard of proof for obtaining a court order for electronic pen register and trap and trace devices is so low, the process of obtaining the court order is basically pointless—rarely will the court order be denied, if ever. *See Limits Judicial Oversight*, *supra* note 154.

301. *See id.*

302. *See supra* Part II.D.2–3 (discussing OCCSSA and FISA).

303. *See supra* Part II.A (discussing Fourth Amendment requirements).

304. *See supra* Part II.A (discussing the requirement to obtain a warrant supported by probable cause for each search and seizure).

search warrant.³⁰⁵ The judge issues the order, and law enforcement inserts the places to be searched.³⁰⁶

4. Roving Wiretap Authority is Extended to Include Intelligence Wiretaps

The Fourth Amendment also requires that search warrants specify the particular telephone to be tapped.³⁰⁷ Prior to the USA PATRIOT Act, roving wiretaps were not allowed for FISA surveillance³⁰⁸ but were allowed for criminal investigations.³⁰⁹ Congress specified, however, that before authorities could activate roving surveillance of a particular telephone line, law enforcement officers needed to demonstrate that the target of the surveillance was actually using the line.³¹⁰

FISA may be used when there is also a criminal investigatory purpose, but only when the primary purpose for initiating the surveillance is that of gathering foreign intelligence.³¹¹ Section 206 of the USA PATRIOT Act extends roving wiretap authority to “intelligence” wiretaps.³¹² This section does not have the same built-in safeguard that is in place for criminal roving wiretaps because law enforcement officials do not have to demonstrate that the target is actually using the phone to be tapped.³¹³ By allowing authorities

305. See *supra* Part III.B.2 (discussing limited requirements of judicial oversight); *Limits Judicial Oversight*, *supra* note 154.

306. See *supra* Part III.B.2 (discussing limited requirements of judicial oversight). This makes the target of a search less able to challenge the search in court. *Limits Judicial Oversight*, *supra* note 154. For example, “[i]f a small ISP in San Francisco thinks that the FBI is illegally viewing content based on a pen register or trap and trace court order issued in New York, it would have to . . . fight the warrant in New York.” *Id.*

307. See *supra* Part II.A (discussing the Fourth Amendment).

308. See *supra* Part II.D.3 (discussing roving wiretaps and FISA surveillance).

309. See *supra* Part II.D.3. See generally *Limits Judicial Oversight*, *supra* note 154.

310. See 18 U.S.C. § 2518(3)(d) (2000).

311. *EPIC Analysis*, *supra* note 275. “The [new legislation] would permit the government to use the FISA procedures in all criminal investigations of international terrorism or espionage and would destroy the distinction, which made the lower standards of FISA constitutional in the first place.” Kate Martin, *Federal Law Enforcement and Intelligence Provisions in Proposed Anti-Terrorism Bill*, available at <http://www.cdt.org/security/011001cnss.pdf> (last visited Oct. 1, 2001).

312. See *supra* Part III.B.2 (discussing the government’s increased ability to obtain roving wiretaps under the USA PATRIOT Act). Intelligence wiretaps are those used in gathering intelligence in formation for national security purposes, as opposed to information gathered for criminal investigations. Compare FISA, 50 U.S.C. §§ 1801–1863 (1999), with AEDPA, Pub. L. No. 104-132, 110 Stat. 1214 (1996).

313. See *supra* Part III.B.2 (discussing the lack of judicial oversight of roving wiretaps under the USA PATRIOT Act); see also *Limits Judicial Oversight*, *supra* note 154. For example, “if a terrorist was using the Internet connection at a public library and law enforcement was using a FISA wiretap order to monitor his Internet communications, it might continue to monitor all

greater latitude in tapping phone lines, the Act places innocent individuals at risk for intrusive government surveillance.³¹⁴ This provides the government with power too broad to go unregulated by judicial oversight.³¹⁵

5. Delayed Notice of Search Warrants Violates the Fourth Amendment

When notice of a search is not provided, the subject of the search has no ability to point out problems or irregularities with the warrant or that law enforcement may be searching beyond what is authorized by the warrant.³¹⁶ Therefore, an innocent person may be victimized by the government and have no ability to protect himself.³¹⁷

Section 213 of the USA PATRIOT Act amends FISA to greatly expand the government's authority to conduct secret or covert searches by relaxing the notice requirement, thus violating privacy protections set forth in the Fourth Amendment.³¹⁸ Usually, notification is required when law enforcement agents conduct a search, except in very specific circumstances when authorities must obtain judicial permission to delay notification.³¹⁹ Section 213 allows the government to request delayed notification of searches in every criminal case.³²⁰ This delayed

Internet communications at that site after the terrorist left and was no longer using the computer," potentially invading the privacy of innocent users. *Limits Judicial Oversight*, *supra* note 154; *EPIC Analysis*, *supra* note 275. "Upon the suspicion that an intelligence target might use such a facility, the FBI could monitor all communications at the facility." *EPIC Analysis*, *supra* note 275. Roving wiretap orders could potentially affect all persons "access[ing] the Internet through public facilities such as libraries, university computer labs and cybercafes." *Id.*

314. See *ACLU Legislative Analysis*, *supra* note 11.

315. *Id.*

316. See Testimony of Timothy H. Edgar, *supra* note 273. For example, the target may be able to show "that the police are at the wrong address, or that the warrant is limited to a search for a stolen car; therefore, the police have no authority to be looking in dresser drawers." *Id.* "The major rationale for requiring a warrant before conducting a search is to ensure that a neutral and detached third person . . . will review a warrant prior to issuance. The invasion of privacy must be held to a minimum." *Id.*

317. *Id.*

318. See *supra* Part III.B.3 (discussing the delayed notice under section 213 of the USA PATRIOT Act). "This means that the government could enter a house, apartment or office with a search warrant when the occupant was away, search through her property and take photographs, and in some cases seize physical property and electronic communications, and not tell her until later." Testimony of Timothy H. Edgar, *supra* note 273.

319. See *supra* notes 262, 277 and accompanying text (discussing the Fourth Amendment's notice requirement).

320. See *supra* Part III.B.3 (discussing delayed notice under § 213 of the USA PATRIOT Act); see also *Expands Sneak and Peak Warrants*, *supra* note 268.

notification, however, is not limited to investigations of terrorist activity.³²¹

The Supreme Court has consistently recognized that the Fourth Amendment requires notice of searches in order to protect against unreasonable searches and seizures.³²² Furthermore, because information gained for purposes of foreign surveillance can be used in a subsequent criminal prosecution, without notice of this surveillance, the target would possibly have no defense regarding the legality of the search.³²³ The distinctions between the two types of surveillance have virtually disappeared,³²⁴ resulting in dissolution of the purpose of enacting two separate surveillance authority statutes, the OCCSSA and FISA.³²⁵

B. The USA PATRIOT Act Overly Expands the Sharing of Sensitive Information Between Intelligence Agencies and Law Enforcement.

Prior law prohibited the disclosure of OCCSSA surveillance intercepts, confidential information gathered in a criminal investigation, and disclosure of grand jury information from law enforcement authorities to intelligence-gathering agencies.³²⁶ When FISA was enacted, the role of the CIA in gathering foreign intelligence within the United States was clarified because the leading role in this intelligence-gathering rested with the Department of Justice.³²⁷ The USA PATRIOT

321. See *supra* Part III.B.3; see also *EPIC Analysis*, *supra* note 275 (discussing delayed notice provision of section 213 of the proposed Anti-Terrorism Act of 2001).

322. See *supra* note 272 and accompanying text (discussing the Fourth Amendment notice requirement); see also *Expands Sneak and Peak Warrants*, *supra* note 268. The Supreme Court has not ruled on the constitutionality of secret searches. See *supra* Part II.B.3.

323. See *supra* Parts III.B.1, III.B.3 (discussing how information can be disclosed to law enforcement and the notice requirement under the USA PATRIOT Act).

324. See *supra* Part III.B.1 (discussing how information can be shared between intelligence agencies and law enforcement).

325. The purpose was to distinguish between the type of surveillance allowed for criminal investigations and that allowed for foreign intelligence surveillance. See *supra* note 88 and accompanying text (discussing the distinction between the requirements of OCCSSA and FISA).

326. FED. R. CRIM. P. 6 (2000). "A grand juror . . . or any person to whom disclosure is made . . . shall not disclose matters occurring before the grand jury, except as otherwise provided for in these rules." *Id.* at 6(e)(2). For a list of exceptions to the rule against disclosure of grand jury information, see FED. R. CRIM. P. 6(e)(3)(A)–(E) (2000). Disclosure to intelligence gathering agencies is not included in this list. FED. R. CRIM. P. 6(e)(3)(A)–(E) (2000); see also *USA PATRIOT Act and the CIA*, *supra* note 201; Rachel King, *Statement on Anti-Terrorism Act of 2001* (Sept. 24, 2001), at <http://www.aclu.org/congress/L092401a.html>; Martin, *supra* note 281.

327. See *supra* Part II.D.3 (discussing the Attorney General's role under FISA); see also *USA PATRIOT Act and the CIA*, *supra* note 201 (noting that after the Church Committee reported CIA abuses of its domestic intelligence gathering capabilities, this power was greatly restricted).

Act blurs this role, giving the CIA increased power to gather intelligence on United States persons³²⁸ and placing power in the hands of the CIA Director to manage domestic intelligence-gathering agencies.³²⁹

1. The USA PATRIOT Act Gives the CIA Too much Power to Gather Intelligence on United States Persons.

In order to protect the privacy of innocent persons, certain information should not be shared between law enforcement and intelligence agencies unless there is a reasonable belief that it is imperative for the national defense or security of the United States.³³⁰ Section 203 of the USA PATRIOT Act allows law enforcement agencies to share sensitive information gathered in criminal investigations with the CIA, NSA, and other federal agencies.³³¹ Section 203(b) permits law enforcement officers to share OCCSSA intercepts of telephone and Internet conversations, also without a court order.³³² Furthermore, section 203(d) permits the sharing of any foreign intelligence or counter-intelligence information obtained as part of a criminal investigation to be disclosed to federal intelligence agencies.³³³ Likewise, section 203(a) allows law enforcement agents to provide foreign intelligence and counter-intelligence information that is revealed to a grand jury to federal intelligence agencies without a court order.³³⁴ All three sections redefine foreign intelligence information to permit more liberal sharing of information about United States citizens, whether or not the information is necessary to protect against terrorist attacks or to guard the national security of the United States.³³⁵

Law enforcement's ability to share information revealed to a grand jury to intelligence-gathering agencies is of particular concern, because

328. See *supra* Part III.B.1 (arguing that the CIA's role is overly expanded, blurring the lines between criminal and intelligence investigations).

329. *Id.* (arguing that the Director of the CIA's powers are too broad).

330. See *USA PATRIOT Act and the CIA*, *supra* note 201.

331. See *supra* Part III.B.1 (discussing how the section allows such sharing and expands the ability of agencies to gather and disclose information). "Other federal agencies" include the INS, the Secret Service, and the Department of Defense. *USA PATRIOT Act and the CIA*, *supra* note 201.

332. *USA PATRIOT Act and the CIA*, *supra* note 201.

333. *Id.*

334. *Id.*

335. See *supra* note 231 (defining foreign intelligence information for the purposes of section 203). Previously, information could be shared only if the information was absolutely necessary to protect the security of the United States. See *USA PATRIOT Act and the CIA*, *supra* note 201.

many people who are investigated by the grand jury are not indicted.³³⁶ The secrecy normally provided for grand jury investigations protects “the integrity of the criminal investigation,” as well as “the privacy and reputation of a person under investigation.”³³⁷ By allowing such liberal sharing of information gained through grand jury investigations, section 203(a) of the USA PATRIOT Act circumvents these protections, which have always been an integral part of the criminal justice system.³³⁸

Section 203 expands the list of people who can access private information, expands the role of the CIA in domestic intelligence-gathering, and expands how the information can be used.³³⁹ While there may be specific times when some sharing of information may be appropriate, allowing the substantial sharing of information, whether criminal intelligence or national security intelligence, blurs the roles of the agencies, which were created for very distinct purposes.³⁴⁰ Without appropriate safeguards, blurring of roles could lead to significant abuses of power.³⁴¹

2. The Director of the CIA is Granted Too Much Power to Manage Domestic Intelligence Gathering

To effectively combat terrorism, law enforcement authorities and intelligence agencies must be able to work together. However, the USA PATRIOT Act opened the door for significant abuse of certain civil liberties of American citizens.³⁴² Prior to the enactment of the USA PATRIOT Act, the Attorney General, as head of the Department of Justice, was responsible for managing domestic intelligence-gathering.³⁴³ While the Attorney General technically maintains this role, section 901 of the USA PATRIOT Act gives part of this power to

336. See King, *supra* note 326. Disclosure to government personnel is allowed only when “deemed necessary by an attorney for the government to assist an attorney for the government in the performance of such attorney’s duty to enforce the criminal law.” FED. R. CRIM. P. 6(e)(3)(iii) (2000).

337. See King, *supra* note 326; see also FED. R. CRIM. P. 6(e)(2) (2000).

338. See King, *supra* note 326; see also *USA PATRIOT Act and the CIA*, *supra* note 201 (discussing how previously protected information may now be exposed).

339. See King, *supra* note 326.

340. *Id.* As King stated, “[s]haring information from criminal cases to intelligence, military and immigration authorities blurs the functions of the various organizations, risks violating the principle of keeping the military out of civilian law enforcement and risks violating the privacy of persons under investigation.” *Id.*

341. See *USA PATRIOT Act and the CIA*, *supra* note 201.

342. *Id.*; *ACLU Legislative Analysis*, *supra* note 11; Halperin & Martin, *supra* note 282.

343. See *supra* notes 112-16 (discussing the roles of the Attorney General and the FBI).

the Director of the CIA.³⁴⁴ Furthermore, the Attorney General, and any other federal law enforcement agency head, is mandated to expeditiously disclose any foreign intelligence information obtained in the course of a criminal investigation to the Director of the CIA.³⁴⁵

Allowing the Director of the CIA to designate information to be collected under FISA puts the Director in a much stronger position to control domestic surveillance information.³⁴⁶ Since the creation of the CIA, Congress has acted to distinguish among law enforcement, the collection of information on Americans and others to be used in criminal prosecutions, and foreign intelligence information.³⁴⁷ Law enforcement and intelligence-gathering agencies have different objectives, requiring different rules, guidelines, and abilities.³⁴⁸ When these boundaries blur, abuses occur.³⁴⁹ The fact that two separate pieces of legislation, OCCSSA and FISA, were enacted to specify when surveillance such as wiretapping is allowed for criminal investigations, and when it is allowed for foreign intelligence gathering, indicates how important the distinction is between the abilities of law enforcement and intelligence-gathering agencies.³⁵⁰ This distinction must be maintained through congressional and judicial oversight.³⁵¹

344. Section 901 of the USA PATRIOT Act states that the Director of the CIA shall "establish requirements and priorities for foreign intelligence information to be collected under the [FISA]." See *supra* Part III.B.1 and notes 239-44 (discussing the roles of the Attorney General and the Director of the CIA); see also *USA PATRIOT Act and the CIA*, *supra* note 201.

345. See *supra* Part III.B.1 and notes 232-33 (discussing section 905 of the USA PATRIOT Act).

346. See *supra* Part III.B.3 (discussing the role of the Director of the CIA); see also *USA PATRIOT Act and the CIA*, *supra* note 201; *ACLU Legislative Analysis*, *supra* note 11.

These information sharing authorizations and mandates effectively put the CIA back in the business of spying on Americans: Once the CIA makes clear the kind of information it seeks, law enforcement agencies can use tools like wiretaps and intelligence searches to provide data to the CIA. In fact, the law specifically gives the Director of Central Intelligence . . . the power to identify domestic intelligence requirements.

ACLU Legislative Analysis, *supra* note 11.

347. See *supra* Part II.A (discussing Constitutional limitations on the collection of information); see also Halperin & Martin, *supra* note 282 (discussing the potential problems with giving this power back to the CIA).

348. See Halperin & Martin, *supra* note 282.

349. See *id.*

350. See *supra* Part II.D.2-3 (discussing OCCSSA and FISA).

351. See *infra* Part V (proposing strong oversight for the implementation of surveillance authorized by the USA PATRIOT Act).

V. PROPOSAL

Increased surveillance capabilities will not provide increased security if they are overly broad and lack judicial review, or if fundamental civil liberties of the American people are diminished.³⁵² Security and civil liberties do not have to be at odds. In a moment of crisis, Congress acted too quickly to reassure the American people.³⁵³ Generally, legislation as detailed as the USA PATRIOT Act takes, at minimum, months to pass, and generally only after significant debate.³⁵⁴ Instead, the USA PATRIOT Act was enacted in six weeks.³⁵⁵ In order to protect American civil liberties, the USA PATRIOT Act must be limited to genuine cases of terrorism.³⁵⁶ Furthermore, Congress must closely and carefully evaluate the actions of the law enforcement and intelligence communities as they begin to use the new rules set forth by the USA PATRIOT Act, and amend the Act accordingly in order to protect civil liberties.³⁵⁷ If Americans lose the rights they hold as free citizens, regardless of how we counteract terrorism and protect ourselves, the terrorists win.³⁵⁸

A. The Changes Made by the Act Must be Strictly Limited to Genuine Cases of Terrorism

The changes made by Title II of the USA PATRIOT Act, including the increased wiretapping ability, covert searches, and the broadened role of the CIA, must be strictly limited to genuine cases of terrorism, or

352. See *supra* Part IV (discussing the effect of the USA PATRIOT Act); see also Amy Bach, *Security With Liberty: A Forum*, at <http://www.thenation.com> (Nov. 1, 2001) (statement of James X. Dempsey); see *supra* Part III.A (discussing the historical development of the USA PATRIOT Act).

353. See *supra* note 224 and accompanying text (discussing the fact that Congress enacted this legislation within six weeks of the September 11th attacks). The actions of the law enforcement and intelligence communities should be closely watched over the next four years, and the sections of the USA PATRIOT Act that do sunset should be re-evaluated at length prior to being re-enacted. See *supra* note 272 (mentioning how certain provisions sunset).

354. See *supra* note 224 and accompanying text (comparing the time frame it took to enact the USA PATRIOT Act with that of the AEDPA).

355. See Krim & O'Harrow, *supra* note 218; Lancaster, *supra* note 220 (detailing the enactment of the USA PATRIOT Act).

356. See *infra* Part V.A (discussing the need to limit the USA PATRIOT Act to genuine cases of terrorism).

357. See *infra* Part V.B (discussing the need for Congress to closely supervise both the Attorney General and director of the CIA).

358. See generally *Enables Law Enforcement*, *supra* note 276 (discussing how the USA PATRIOT Act expands law enforcement's ability to "spy" on Americans); *Limits Judicial Oversight*, *supra* note 154 (discussing how the USA PATRIOT Act limits judicial oversight in the area of wiretapping);

abuses will occur.³⁵⁹ As long as limitations are applied, the expansion of the surveillance powers contained in the USA PATRIOT Act should not be in opposition to the rights of the American people.³⁶⁰ The USA PATRIOT Act, however, ignores abuses of the past when only minimal judicial review was required.³⁶¹ After all, it was Congress' growing concern with protecting the privacy rights of the American people and providing improved congressional and judicial oversight of the intelligence community that led to the enactment of the Federal Communications Act of 1934, OCCSSA, and FISA.³⁶²

B. Congress and the Courts Must Closely Supervise the Actions of the Attorney General and the Director of the CIA.

In order to protect American civil liberties and abide by Fourth Amendment requirements, Congress must establish strict guidelines for gathering and disseminating information gathered under the USA PATRIOT Act.³⁶³ Furthermore, courts must take an active role in enforcing Fourth Amendment protections.³⁶⁴ Likewise, strict standards for filtering content obtained from Internet communications must be established.³⁶⁵ Finally, specificity should be required for search warrants,³⁶⁶ and notice should be provided at all times unless exigent circumstances exist.³⁶⁷

359. See *Limits Judicial Oversight*, *supra* note 154; *supra* Part IV (discussing the potential disregard for Fourth Amendment protections from unwarranted government intrusion and expanded intelligence powers); see also *ACLU Legislative Analysis*, *supra* note 11.

360. See Morton H. Halperin, *Less Secure, Less Free*, AMERICAN PROSPECT, Nov. 19, 2001, at 10, available at <http://www.prospect.org/print/V12/20/halperin-m.html> (Nov. 19, 2001).

361. See *supra* Part IV (describing how the USA PATRIOT act was passed as a hasty response to September 11, 2001). For example, potentially anyone who protests the attacks on Afghanistan could be investigated under the guise of counterintelligence, when all they are doing is asserting their right to protest. Halperin, *supra* note 360.

362. See *supra* Part II.D (discussing the history of domestic and foreign intelligence legislation). But see Statement of Sen. Leahy, *supra* note 230 (discussing the positive aspects of breaking down barriers between law enforcement and foreign intelligence).

363. See *infra* Part V.B.1 (discussing measures to limit the scope of the act's power to gather and disseminate acquired information).

364. See *infra* Part V.B.2 (discussing the need for the Supreme Court to consider the Fourth Amendment ramifications of the act).

365. See *infra* Part V.B.3 (suggesting greater judicial vigilance when authorizing electronic surveillance).

366. See *infra* Part V.B.3 (proposing that the Fourth Amendment must require specificity in order to grant a warrant).

367. See *infra* Part V.B.4 (discussing the notice requirement of the Fourth Amendment for searches and seizures).

1. Strict Guidelines for the Gathering and Dissemination of Information Must be Established

Under the strictest of safeguards, the sharing of information between law enforcement and intelligence agencies may be appropriate.³⁶⁸ Regardless of the situation, this sharing should occur only when it is absolutely necessary.³⁶⁹ Furthermore, the Senate Judiciary Committee must play an active role in ensuring that these protections are upheld, maintaining a close working relationship with the Attorney General and the Director of the CIA.³⁷⁰ Two necessary safeguards are court approval of such sharing and limiting the information shared to foreign intelligence information.³⁷¹

The USA PATRIOT Act does provide that information disclosed by a grand jury should be filed under seal with the court,³⁷² stating that information was disclosed and to what agency, department, or entity it was disclosed.³⁷³ Furthermore, the USA PATRIOT Act requires that the Attorney General establish procedures to regulate the disclosure of information derived from wiretaps and grand juries.³⁷⁴ Records should be kept of all disclosures made, and the intelligence community should be required to produce documentation of such disclosures to Congress if necessary.

2. The Courts Must Take an Active Role in Enforcing Protections Guaranteed by the Fourth Amendment

The Supreme Court has not addressed the issue of a national security exception for warrantless foreign intelligence gathering.³⁷⁵ The Court should address this issue and establish, at a minimum, that the

368. See *USA PATRIOT Act and the CIA*, *supra* note 201; *ACLU Legislative Analysis*, *supra* note 11.

369. See King *supra* note 326; *USA PATRIOT Act and the CIA*, *supra* note 201; *supra* Part IV.B (discussing the only circumstances when information sharing should be allowed).

370. See King, *supra* note 327; 147 Cong. Rec. S10990 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

371. See Halperin & Martin, *supra* note 282.

372. USA PATRIOT Act § 203, Pub. L. No. 107-56, 115 Stat. 272 (2001). "Within a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made." *Id.* § 203(a)(V)(iii).

373. See *id.*; 147 CONG. REC. S10090-93 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

374. USA PATRIOT Act § 203(c); see *supra* note 238 and accompanying text (discussing how the Attorney General is required to establish guidelines for the disclosure of such information).

375. See Banks & Bowman, *supra* note 28, at 91-92 (noting that the Supreme Court has yet to resolve this issue); *supra* note 92 and accompanying text (detailing cases involved in unresolved circuit splits on the issue).

reasonableness requirement of the Fourth Amendment is applicable.³⁷⁶ Setting this standard will assist in protecting those who exercise their First Amendment rights of free speech and freedom of association, but who are not a threat to national security, from unwarranted governmental intrusion.³⁷⁷ Furthermore, the Court should be consistent in applying a warrantless search standard to instances of both domestic and foreign intelligence gathering.³⁷⁸

3. Strict Judicial Oversight Should be Required for Electronic Surveillance

Because the USA PATRIOT Act does not provide guidelines describing how the intelligence community should avoid collecting content through the use of pen registers and trap and trace devices³⁷⁹ for internet surveillance, the Attorney General and the Director of the CIA must work together to establish realistic methods for filtering this information.³⁸⁰ Information in the subject line of an e-mail provides more information than a number dialed on a telephone, because it potentially yields personal, private information that may be unnecessary to the investigation.³⁸¹ The judge issuing the pen register or trap and trace warrant must also investigate the information to be obtained, and require a showing that the monitored communications are truly those of the surveillance target.³⁸²

Furthermore, the Fourth Amendment requires that when a search warrant is issued, the person or place to be searched must be specified.³⁸³ Although not a general restraint on all police practices, requiring that a warrant name a specific place or person to be searched

376. See *Katz v. United States*, 389 U.S. 347 (1967) (Harlan, J., concurring) (setting forth a two-part test to determine whether a search or seizure is reasonable); *supra* Part II.A.2 (discussing the reasonableness requirement).

377. See *supra* Part II.A–B (discussing the rationale behind both the Fourth Amendment and the enactment of national security legislation); see also Halperin, *supra* note 360.

378. See *Zweibon v. Mitchell*, 516 F.2d 594, 613–14 (D.C. Cir. 1975) (stating in dicta that all warrantless electronic surveillance is unreasonable, whether for domestic or foreign intelligence gathering purposes).

379. See *supra* note 247 (providing definitions of trap and trace devices).

380. See 147 CONG. REC. S10992, (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) (noting that the USA PATRIOT Act breaks down traditional barriers between law enforcement and foreign intelligence).

381. See *Limits Judicial Oversight*, *supra* note 154.

382. See USA PATRIOT Act §§ 216, 206, Pub. L. No. 107-56, 115 Stat. 272 (2001); *Limits Judicial Oversight*, *supra* note 154.

383. See FED. R. CRIM. P. 41(c)(1) (2000); *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *Terry v. Ohio*, 392 U.S. 1, 20 (1968) (requiring police to obtain a search warrant whenever practicable).

is another important protection from unwarranted governmental intrusion, and should be reaffirmed by the Supreme Court, even in the context of foreign intelligence gathering.³⁸⁴ The Framers of the Constitution, in enacting the Fourth Amendment, wanted to ensure that Americans were not subjected to intrusions similar to that allowed by the British general warrant.³⁸⁵ At a minimum, when a blank warrant is issued, the requesting officer or agent should be required to report back to the judge within twenty-four hours of initiating surveillance.³⁸⁶

4. Notice Should be Required

Finally, in criminal proceedings, the Fourth Amendment requires that notice of a search and seizure be given to the target of the activity.³⁸⁷ When this practice is ignored, it is a violation of the Fourth Amendment and should be recognized as such by the Courts.³⁸⁸ The USA PATRIOT Act authorizes delay of this notice requirement in a variety of circumstances, including criminal proceedings.³⁸⁹ Under FISA, the target of foreign intelligence surveillance may never be given notice of the search for the legitimate purpose of protecting national security.³⁹⁰ One purpose behind the separate enactment of OCCSSA and FISA was to keep the issues of criminal surveillance separate from that of foreign intelligence gathering.³⁹¹ Delaying notice of search warrants under the USA PATRIOT Act blurs that line and should not be allowed.³⁹²

VI. CONCLUSION

The United States has a long history of balancing the importance of protecting national security against maintaining the constitutionally

384. See *Zweibon v. Mitchell*, 516 F.2d 594, 613-14 (D.C. Cir. 1975) (stating in dicta, warrant requirements should be applied to foreign intelligence gathering).

385. See *Banks & Bowman*, *supra* note 28, at 2-3 (discussing historical background of the Fourth Amendment).

386. See *Limits Judicial Oversight*, *supra* note 154 (discussing the need to set guidelines for judicial oversight of blank warrants).

387. See *supra* Part II.B (discussing the holding of *Katz v. United States*, that the Fourth Amendment applies to persons, not just property). Notice of a search may be delayed only to avoid compromising an ongoing investigation or form some other good reason. *United States v. Villegas*, 899 F.2d 1324, 1336-37 (2d Cir. 1990); see *supra* note 262 and accompanying text (discussing Fourth Amendment notice requirement).

388. See *supra* Part II.B (discussing the Fourth Amendment's application to criminal investigations).

389. See USA PATRIOT Act § 213, Pub. L. No. 107-56, 115 Stat. 272 (2001).

390. See *Enables Law Enforcement*, *supra* note 276 (discussing the delay of notice provisions).

391. See *id.*

392. See *id.*

protected freedoms enjoyed by its citizens. Sometimes, certain liberties must be temporarily sacrificed in order to protect the country. However, when those liberties are permanently sacrificed, the purpose of the Constitution and the objective of the Founding Fathers are negated, and the United States ceases to be a country of freedom and protected civil liberties. In enacting the USA PATRIOT Act of 2001, Congress overreached its power and provided the tools to take away important American civil liberties. To rectify this wrong, Congress must strictly monitor the actions of law enforcement and intelligence agencies, amending certain sections of the Act in order to both protect the nation and uphold the Constitution.