Notre Dame Journal of Law, Ethics & Public Policy

Volume 19
Issue 1 *Symposium on Security & Liberty*

Article 21

February 2014

From the Purpose to a Significant Purpose: Assessing the Constitutionality of the Foreign Intelligence Surveillance Act under the Fourth Amendment

Jennifer L. Sullivan

FROM "THE PURPOSE" TO "A SIGNIFICANT PURPOSE": ASSESSING THE CONSTITUTIONALITY OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT UNDER THE FOURTH AMENDMENT

JENNIFER L. SULLIVAN*

This Note is a critical commentary on the state of foreign intelligence surveillance for national security purposes since the terrorist attacks of September 11, 2001. In particular, it addresses the constitutionality of the Foreign Intelligence Surveillance Act of 1978 ("FISA") under the Fourth Amendment as modified by the amendments enacted in the USA PATRIOT Act of 2001 ("Patriot Act").[1] In this Note, I propose that FISA, as amended by section 218 of the Patriot Act, is constitutional because it violates neither the Warrant Clause nor the Reasonableness Clause of the Fourth Amendment.

FISA does not violate the Warrant Clause because FISA court orders fulfill the lawful requirements of a warrant: issuance by a neutral and disinterested judge, presence of a probable cause standard, and a particularized account of the locations to be searched, and the objects and items to be seized. In addition, FISA does not violate the Reasonableness Clause on two distinct grounds. First, FISA qualifies under the "special needs" exception to the Fourth Amendment because the prevention of terrorist attacks like September 11th that pose significant damage and injury is the sort of action that far surpasses the normal role of law enforcement. Second, FISA also satisfies the criteria for a limited national security exception to the Fourth Amendment. Although the Supreme Court has not determined whether a national security exception to the Fourth Amendment exists, this foreign intelligence exclusion has been endorsed by many federal circuit courts of appeal. Further support for the exception stems from the President's traditionally broad discretion in the area of foreign affairs, and the fact that, after September 11th, public policy dictates that the need to protect the United States

* J.D. Candidate, University of Notre Dame Law School, 2005; Thomas J. White Scholar 2003–2005; B.A., Harvard University, 2001. Special thanks to Professor G. Robert Blakey for his assistance in the formation of this Note.

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

from future terrorist attacks far outweighs overstated concerns regarding individual civil liberties. Thus, the Patriot Act amendments to FISA are vital to ensuring American national security after September 11th, and these modifications of FISA are constitutional under the Fourth Amendment.

INTRODUCTION

On September 11, 2001, the United States suffered the most devastating attacks on American soil since the assault on Pearl Harbor during World War II.[2] In the span of one short hour, nineteen al Qaeda terrorists crippled the economic and military hubs of the United States by hijacking and crashing four commercial airplanes into the Twin Towers of New York's World Trade Center, the Pentagon, and a field southeast of Pittsburgh, Pennsylvania.[3] The consequences of the September 11th terrorist attacks were staggering: approximately three thousand innocent casualties,[4] the obliteration of a symbolic national skyline, and the frightening realization that it has become "increasingly easy to plan and implement highly destructive terrorist actions in the territory of another state."[5]

The September 11th terrorist attacks underscored the inadequacies of the legislation that had been enacted to combat terrorism in the wake of the Oklahoma City bombing. Five years before September 11th, critics of the Antiterrorism and Effective Death Penalty Act of 1996 ("AEDPA") prophetically stated, "Congress passed a weak shadow of the original bills, which respond[ed] too broadly to earlier charges of extremism and is likely to do little to stop terrorism."[6] In an effort to bolster the

2. *See Latest Additions to Victims List*, AP ONLINE, Feb. 5, 2002, 2002 WL 11688056 (stating that 2,759 deaths had been confirmed in the terrorist attacks of September 11th).

3. Michael Grunwald, *Terrorists Hijack 4 Airliners, Destroy World Trade Center, Hit Pentagon; Hundreds Dead; Bush Promises Retribution; Military Put on Highest Alert*, WASH. POST, Sept. 12, 2001, at A1.

4. *See* Matthew C. Weibe, Comment, *Assassination in Domestic and International Law: The Central Intelligence Agency, State-Sponsored Terrorism, and the Right of Self-Defense*, 11 TULSA J. COMP. & INT'L L. 363, 363 (2003).

5. W. Michael Reisman, *International Legal Responses to Terrorism*, 22 HOUS. J. INT'L L. 3, 4 (1999).

6. Note, *Blown Away? The Bill of Rights after Oklahoma City*, 109 HARV. L. REV. 2074, 2091 (1996). The author argues that the original proposed legislation after the Oklahoma City tragedy raised concerns about individual civil liberties but was still constitutional legislation. *Id.* The unwarranted concerns about reduced civil liberties resulted in a version of the Antiterrorism and Effective Death Penalty Act of 1996 ("AEDPA") that failed to make any significant changes to the Federal Bureau of Investigation's surveillance powers. *Id.* at 2079.

existing inadequate antiterrorism legislation, Congress quickly passed the Patriot Act six weeks after the September 11th attacks.[7] This legislation, which has been criticized by civil liberties groups as unconstitutionally infringing on individual privacy rights,[8] attempts to provide domestic law enforcement and intelligence agencies with broad powers to fight terrorism and protect national security interests.[9]

One of the most controversial aspects of the Patriot Act is the fact that several provisions significantly "increase the government's authority and ability to monitor wire and electronic communication."[10] Specifically, section 218 of the Patriot Act amended the Foreign Intelligence Surveillance Act of 1978 ("FISA") by lowering the threshold required to conduct surveillance for national security purposes.[11] While authorization for a FISA court order traditionally entailed certification that "the purpose" of the surveillance was to acquire foreign intelligence,[12] section 218 allows the FISA court to issue a FISA warrant if "a significant purpose" of the investigation is foreign intelligence surveillance.[13] Critics argue that this seemingly innocuous legislation violates the Fourth Amendment by permitting law enforcement officials to employ the lower probable cause standard of

7. The Senate passed the Patriot Act on October 25, 2001, and it was signed into law by President Bush on October 26, 2001.

8. *See* Press Release, American Civil Liberties Union, ACLU Calls for Monitoring of USA Patriot Act (Jan. 24, 2002), *at* http://www.aclu.org/NationalSecurity/NationalSecurity.cfm?ID=9710&c=111 (on file with the Notre Dame Journal of Law, Ethics & Public Policy); Press Release, Center for Democracy and Technology, CDT Urges Congress to Move Forward with Legislation to Fix the Patriot Act (Oct. 14, 2003), *at* http://www.cdt.org/press/031014press.shtml (on file with the Notre Dame Journal of Law, Ethics & Public Policy).

9. *See* Jonathan Krim & Robert O'Harrow, Jr., *Bush Signs into Law New Enforcement Era; U.S. Gets Broad Electronic Powers*, WASH. POST, Oct. 27, 2001, at A06. According to Krim and O'Harrow, the Patriot Act eases the difficulties of conducting searches and detaining or deporting suspects of terrorist activity, as well as allows law enforcement and intelligence to monitor financial transactions and internet communications of targeted individuals. *See id.*; *see also* U.S. DEP'T OF JUSTICE, THE USA PATRIOT ACT: PRESERVING LIFE AND LIBERTY, *at* http://www.lifeandliberty.gov/patriot_overview_pversion.pdf (last visited Mar. 1, 2005) (on file with the Notre Dame Journal of Law, Ethics & Public Policy).

10. Heath H. Galloway, Note, *Don't Forget What We're Fighting For: Will the Fourth Amendment Be a Casualty of the War on Terror?*, 59 WASH. & LEE L. REV. 921, 962 (2002).

11. *See* Patriot Act § 218, 115 Stat. 291 (2001).

12. *See* Tracey Topper Gonzalez, *Individual Rights Versus Collective Security: Assessing the Constitutionality of the USA Patriot Act*, 11 U. MIAMI INT'L & COMP. L. REV. 75, 109 (2003).

13. *See* 50 U.S.C.A. § 1804(a)(7)(b) (2003).

FISA court orders to surveillance in standard criminal investigations.[14]

However, this constitutional analysis of the Patriot Act amendments to FISA is flawed. Neither the Warrant Clause nor the Reasonableness Clause of the Fourth Amendment prohibits the executive branch from employing FISA court orders to conduct surveillance of a particular foreign target if a "significant purpose" of the investigation is foreign intelligence. FISA court orders arguably fulfill the three requirements of the Warrant Clause: authorization by a neutral magistrate, probable cause, and particularity.[15] Furthermore, unprecedented levels of terrorist threats cause the balance between national security and civil liberties to reasonably swing in the government's favor. Specifically, the plenary power of the executive branch with respect to foreign affairs,[16] the widespread judicial support for a limited foreign intelligence exception to the Fourth Amendment,[17] and FISA's similarity to legislation regulating criminal investigations[18] help the Patriot Act amendments satisfy the Reasonableness Clause of the Fourth Amendment.

This Note focuses on the constitutionality of FISA under the Fourth Amendment as modified by section 218 of the Patriot Act. Part I reviews the history of warrantless electronic surveillance for the purposes of national security, including the inability of Congress and the Supreme Court to propose and monitor standards regulating the use of such surveillance. Part II discusses the original framework of FISA and the initial foreign intelligence purpose standard. Part III explores the Patriot Act and its amendments to FISA, as well as the recent judicial decisions in the FISA court and the Foreign Intelligence Surveillance Court

14. Brief on Behalf of the American Civil Liberties Union et. al. at 24–26, *In re* Sealed Case No. 02-001, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002), *available at* http://archive.aclu.org/court/091902FISCRbrief.pdf (on file with the Notre Dame Journal of Law, Ethics & Public Policy) [hereinafter ACLU Brief]. The ACLU brief was joined by the Center for Democracy and Technology, Center for National Security Studies, Electronic Privacy Information Center, Electronic Frontier Foundation, and Open Society Institute. *Id.*

15. *See* Dalia v. United States, 441 U.S. 238, 255 (1979).

16. *See* 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, 106 (1985).

17. *See* United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); United States v. Butenko, 494 F.2d 593, 596–97 (3d Cir. 1974); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); United States v. Truong Dinh Hung, 629 F.2d 908, 913–16 (4th Cir. 1980).

18. Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351, tit. III, 82 Stat. 211 (codified as amended at 18 U.S.C. §§ 2510–2522 (2000)) [hereinafter Title III].

of Review regarding the constitutionality of FISA's new "significant purpose" standard for foreign intelligence surveillance. Part IV will analyze the constitutionality of the Patriot Act amendments to FISA under the Fourth Amendment. Finally, this paper will conclude that FISA's new "significant purpose" standard, as amended by section 218 of the Patriot Act, violates neither the Warrant Clause nor the Reasonableness Clause of the Fourth Amendment for both analytical and public policy reasons.

I. FOREIGN INTELLIGENCE SURVEILLANCE PRIOR TO FISA

For approximately fifty years prior to the passage of the original Foreign Intelligence Surveillance Act, Congress and the Supreme Court struggled to establish the scope and parameters of electronic surveillance for criminal investigations and foreign intelligence purposes.[19] While Congress ultimately reached a solution with respect to wiretapping for criminal investigations that satisfied the Supreme Court,[20] a definitive standard for national security surveillance has been far more elusive. Several federal circuit courts have deferred to the executive branch of the federal government for the purpose of foreign intelligence wiretapping,[21] but the Supreme Court has refused to resolve the question.[22] The problems inherent in unregulated foreign intelligence surveillance led to the enactment of FISA in 1978.

A. *Traditional Constitutional and Legislative Framework for Electronic Surveillance Under the Fourth Amendment*

The Fourth Amendment of the United States Constitution provides in part that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[23] The Supreme Court was initially presented with the question of whether electronic wiretapping was per se unconstitutional in *Olmstead v. United States*.[24] Speaking for the majority in a sharply divided Court, Chief Justice Taft stated that electronic wiretapping of "voluntary [telephone] conversations secretly overheard" was

19. Gregory E. Birkenstock, Note, *The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis*, 80 GEO. L.J. 843, 846–47 (1992).

20. *See generally* Title III.

21. *See Brown*, 484 F.2d at 426; *Butenko*, 494 F.2d at 596–97; *Buck*, 548 F.2d at 875; *Truong Dinh Hung*, 629 F.2d. at 913–16.

22. *See* United States v. United States District Court (Keith), 407 U.S. 297, 321–22 (1972).

23. U.S. CONST. amend. IV.

24. Olmstead v. United States, 277 U.S. 438 (1928).

admissible in a criminal trial because such surveillance did not constitute an unreasonable search of an "effect" under the Fourth Amendment.[25]

The Court's early acceptance of electronic surveillance as inherently reasonable was short-lived, as Congress placed strict limits on the use of wiretapping in criminal and intelligence investigations. The Federal Communications Act of 1934 attempted to place significant restraints on electronic surveillance by completely prohibiting the interception and use of radio and wire communications,[26] and the Supreme Court held in *Nardone v. United States*[27] that the statutory language of section 605 of the Federal Communications Act of 1934 forbids individuals to intercept or publicly disseminate such electronic surveillance.[28] However, the executive branch of the federal government continued to use electronic wiretapping in certain circumstances by interpreting *Nardone* to prevent such surveillance "only when it was combined with disclosure of its fruits outside of the government."[29] The Federal Bureau of Investigation ("FBI") specifically interpreted section 605 "as only preventing the 'divulgence' of information obtained by wiretapping in court, while not prohibiting wiretapping if the information was not used at trial."[30]

The concern that the United States and its citizens were not being adequately defended during World War II led the executive branch to utilize electronic surveillance tactics for the purposes of national security. Since Congress failed to pass legislation authorizing the use of electronic wiretapping for national security purposes, President Franklin Roosevelt "acted unilaterally and expressed his desire to Attorney General [Robert] Jackson that 'listening devices' be used when 'grave matters involving defense of the nation,' such as espionage or subversion, might be involved."[31] In fact, surveillance of this nature assisted the United States to ultimately defeat Japan during World War II. In 1935, before an official American declaration of war, United

25. *Id.* at 466.

26. Federal Communications Act of 1934, ch. 652, 48 Stat. 1064, 1103–04 (1934) (codified as amended at 47 U.S.C. § 605 (2000)).

27. Nardone v. United States, 302 U.S. 379 (1937).

28. *Id.* at 382.

29. Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 797 (1989).

30. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1139 (2002) (citing WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE 260 (3d ed. 2000)).

31. Cinquegrana, *supra* note 29, at 798.

States Naval Intelligence officers intruded the Washington, D.C., office of the Japanese naval attaché, photographed his secret code machine, and searched the contents of his briefcase.[32] The intelligence gathered from this covert surveillance operation led to the deciphering of the Japanese Naval Code, and supplied Admiral Chester Nimitz of the American Pacific Fleet with vital information to defeat the Japanese army during the Battle of Midway in May 1942.[33] According to Professor G. Robert Blakey, "America's naval forces were distinctly inferior; America's superior intelligence laid the foundation for the victory."[34] Such intelligence practices continued after World War II hostilities ceased, with President Truman's approval of "broader use of electronic surveillance" and the FBI's use of "trespassory electronic surveillance" for issues of national security.[35]

Congress's inability to control the executive branch's exploitation of electronic surveillance in criminal and intelligence investigations gave the Supreme Court the opportunity to reevaluate its property conception of privacy rights under the Fourth Amendment. In *Katz v. United States*,[36] the Court overruled *Olmstead* and held that the Fourth Amendment properly applied to the use of electronic surveillance in the absence of physical trespass.[37] Justice Stewart, speaking for the *Katz* majority, reaffirmed the Court's position that warrantless searches "conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[38] While the Court clarified the point that a warrant is needed to conduct electronic wiretapping for criminal investigations, the *Katz* majority buried its refusal to address the issue of whether a warrant is required for national security surveillance in a footnote.[39] Justice White brought this issue to the forefront in his *Katz* concurrence, stating that the Warrant Clause of the Fourth Amendment should not apply to national security surveillance if the President or Attorney

32. *See* G. Robert Blakey, Concurrence, ELECTRONIC SURVEILLANCE: REPORT OF THE NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE 208 (1976).

33. *See id.*

34. *Id.*

35. Cinquegrana, *supra* note 29, at 798.

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

37. *Id.* at 353–59.

38. *Id.* at 357.

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

General has authorized such searches as constitutionally reasonable.[40]

One year after the *Katz* decision, Congress codified the warrant requirement for electronic surveillance in criminal investigations by ratifying Title III of the Omnibus Crime Control and Safe Streets Act ("Title III").[41] Under Title III, a judge or magistrate may issue a warrant in a criminal case if probable cause exists to believe "that an individual is committing, has committed, or is about to commit a particular offense . . . ."[42] However, Title III's original language indicated that Congress refused to place restrictions on the President's ability to obtain foreign intelligence information, ensure the national security of the United States, and protect the country from aggressive foreign powers.[43] Thus, the original language of Title III demonstrated Congress's recognition of an inherent presidential authority to authorize warrantless searches for the purposes of foreign affairs and national security.[44]

B. *Constitutionality of Warrantless Electronic Surveillance for National Security Purposes*

Because neither *Katz* nor Title III placed any significant restraints on the executive branch's ability to conduct warrantless electronic surveillance for national security purposes, the executive branch operated as if it had "total executive autonomy in devising and implementing surveillance procedures for internal security missions."[45] The President and Attorney General unequivocally possessed this power until the Supreme Court evaluated whether Title III was an implicit grant of authority to the

40. *Id.* at 364.

41. Title III § 802 (codified as amended at 18 U.S.C. § 2518(3)(a) (2000)).

42. 18 U.S.C. § 2518(3)(c).

43. *See* Cinquegrana, *supra* note 29, at 801. The original language of section 2511(3) read as follows: "[N]othing 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 other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, and or to protect national security information against foreign intelligence activities . . . ." *Id.*; *see also* Title III, § 2511(3) (1968) (repealed 1978). Section 2511(3) was repealed in 1978 after the passage of the Foreign Intelligence Surveillance Act.

44. *See* Title III § 802 (codified at 18 U.S.C. § 2511(3) (1968)).

45. Galloway, *supra* note 10, at 940. Galloway argues that Congress and the Supreme Court perpetuated the executive branch's belief that it could conduct warrantless electronic surveillance without judicial review whenever it was imperative to issues of national security. *Id.* at 940–41.

executive branch in matters of national security.[46] In refusing to determine the "scope of the President's surveillance power with respect to the activities of foreign powers,"[47] the Court provided federal circuit courts with the chance to formulate an exception to the Fourth Amendment for issues of foreign intelligence and national security, an opportunity that several courts seized and answered in the affirmative. These judicial decisions ultimately paved the way for the ratification of FISA.

1. *Keith* and the Possibility of a National Security Exception to the Fourth Amendment

While the Supreme Court only briefly discussed the issue of electronic wiretapping for national security purposes in *Katz*, in *United States v. United States District Court (Keith)*, the Court directly confronted the President's constitutional ability to conduct warrantless electronic surveillance in the area of foreign affairs.[48] In *Keith*, the United States charged three defendants with conspiracy to destroy government property.[49] Law enforcement learned of the defendants' plan to bomb a Michigan office of the Central Intelligence Agency ("CIA") by using a wiretap that was authorized by Attorney General John Mitchell but received no prior judicial approval.[50] The Court ruled that warrantless electronic surveillance for the purpose of domestic security is unconstitutional and does not mandate an exception to the requirements of the Fourth Amendment.[51]

Although the *Keith* Court expressly held that electronic surveillance for domestic security purposes requires judicial approval, the Court refused to extend its decision beyond the "domestic aspects of national security."[52] First, the Court acknowledged that Article II of the Constitution[53] implicitly grants the President broad authority in the area of foreign affairs[54] but indicated that Title III neither confers nor restricts

46. United States v. United States District Court (Keith), 407 U.S. 297 (1972).

47. *Id.* at 308.

48. *Id.* at 299.

49. *Id.* at 297.

50. *Id.* at 301.

51. *Id.* at 320.

52. *Id.* at 321.

53. U.S. CONST. art. II. The Presidential Oath requires the President to "preserve, protect, and defend the Constitution of the United States." *Id.* art. II, § 1, cl. 7. *Keith* says that "implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means." *Keith*, 407 U.S. at 308.

54. *Keith*, 407 U.S. at 310.

the ability of the executive branch to conduct national security wiretapping without judicial review.[55] Second, and more importantly, the *Keith* Court recognized that the purposes of ordinary criminal investigations and foreign intelligence surveillance are distinct.[56] Because the government has a compelling interest in the preservation of the national security, Justice Powell reasoned that different standards for national security electronic surveillance "may be compatible with the Fourth Amendment if they are *reasonable* both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[57] Thus, the *Keith* Court recognized that warrantless electronic wiretapping for the purpose of national security is not exempt from the Fourth Amendment but suggested the possibility that such electronic surveillance for foreign intelligence reasons may be constitutional if, by balancing the national security against civil liberties, the interests of the government outweigh the privacy concerns of individual citizens.

2. Lower Court Interpretations of *Keith* and the National Security Exception to the Fourth Amendment

By once again sidestepping the issue of whether national security electronic surveillance conducted without judicial review is constitutional under the Fourth Amendment, the Supreme Court opened the door for a variety of conflicting views regarding wiretapping for foreign intelligence purposes. Although only a handful of federal circuit courts of appeal have addressed the constitutionality of national security wiretapping, an overwhelming majority of those courts deciding the question have held that warrantless electronic surveillance for national security reasons is a reasonable and legitimate exercise of the President's inherent power as Commander in Chief, and qualifies as a foreign intelligence exception to the Warrant Clause of the Fourth Amendment.

One year after the *Keith* decision, the Fifth Circuit addressed the same question that the Supreme Court had previously declined to answer. In *United States v. Brown*,[58] the Fifth Circuit upheld the legality of warrantless electronic wiretapping for the purpose of gathering foreign intelligence.[59] The *Brown* court was

55. *Id.* at 308. According to Justice Powell, nothing in Title III showed an intent to "expand or to contract or to define whatever presidential surveillance powers existed in matters affecting the national security." *Id.*

56. *Id.*

57. *Id.* at 322–23 (emphasis added).

58. 484 F.2d 418, 426 (5th Cir. 1973).

59. *Id.*

careful to note that the President and Attorney General are prohibited from authorizing wiretapping without judicial review in the area of domestic security, but it distinguished the issue of domestic threats to national security from foreign intelligence surveillance. The Fifth Circuit reaffirmed *Brown* in its holding in *United States v. Clay*[60] and held "that the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence."[61]

Shortly after *Brown*, the same question began to appear more frequently in federal circuit courts of appeal across the country. In *United States v. Butenko*,[62] the Third Circuit agreed that warrantless electronic surveillance for the purpose of national security was constitutional. As in *Brown*, the Third Circuit agreed that Article II of the Constitution implicitly authorized the President, through the Attorney General, to broadly conduct foreign intelligence surveillance.[63] Unlike the Fifth Circuit, the *Butenko* court further limited this power by insisting that wiretapping for reasons of national security must be the primary purpose of the investigation, and any information collected relating to criminal proceedings must be incidental to the foreign intelligence inquiry.[64] According to Circuit Judge Adams, "Since the primary purpose of these searches is to secure foreign intelligence information, a judge . . . must, above all, be assured that this was in fact its primary purpose and that the accumulation of evidence of criminal activity was incidental."[65] Thus, the Third Circuit appeared to be more hesitant in supporting a broad foreign intelligence exception to the Fourth Amendment, but did state that the warrant requirement would hinder the executive branch's ability to adequately protect the national security.[66] Four years later, the Ninth Circuit contributed to the burgeoning trend among circuit courts with respect to the constitutionality of foreign intelligence wiretapping. Citing *Clay* and *Butenko*, the Ninth Circuit explicitly held in *United States v. Buck*[67] that the "foreign security wiretaps are a recognized exception to the general warrant requirement [of the Fourth Amendment]."[68]

60. 430 F.2d 165, 170–72 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971).

61. *Brown*, 484 F.2d at 426.

62. 494 F.2d 593 (3d Cir. 1974).

63. *Id.* at 603.

64. *Id.* at 606.

65. *Id.*

66. *Id.* at 604.

67. 548 F.2d 871 (9th Cir. 1977).

68. *Id.* at 875.

In 1980, the Fourth Circuit weighed in on the constitutionality of warrantless foreign intelligence surveillance. In *United States v. Truong Dinh Hung*,[69] the Fourth Circuit considered an appeal from defendants initially convicted of espionage and conspiracy to commit espionage for communicating classified information from the United States to the Socialist Republic of Vietnam during the Paris negotiations in 1977. While the *Truong* court held that the executive branch of the government is not constitutionally required under the Fourth Amendment to obtain a search warrant to conduct electronic surveillance for national security purposes,[70] the Fourth Circuit recognized, as the Third Circuit did in *Butenko*, that the primary purpose of the wiretapping operation must apply to foreign intelligence surveillance instead of criminal investigations. According to Judge Winter, "the executive can proceed without a warrant only if it is attempting primarily to obtain foreign intelligence from foreign powers or their assistants."[71] The Fourth Circuit refused to apply this foreign intelligence exception to criminal investigations because "the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede . . . ."[72] Although the *Truong* court tried to provide a workable guideline as to the constitutionality of warrantless foreign intelligence surveillance, the primary purpose doctrine "added yet another dimension to the vexing problem of how to reconcile the necessities of national security surveillance with the Fourth Amendment."[73]

Despite the popularity of at least a limited foreign intelligence surveillance exception to the Fourth Amendment, one court refused to follow suit. In *Zwiebon v. Mitchell*,[74] the D.C. Circuit ruled that warrantless surveillance used by the Attorney General against the Jewish Defense League ("JDL") to monitor the violent actions the JDL took against Soviet officials in the United States violated the Fourth Amendment.[75] While the majority holding reaffirmed *Keith* by restricting surveillance installed against a domestic organization by the executive branch for the

69. 629 F.2d 908 (4th Cir. 1980). Although Congress passed FISA in 1978, the warrantless electronic surveillance in question in *United States v. Truong Dinh Hung* occurred in 1977 and 1978. *Id.* at 912.

70. *Id.* at 913.

71. *Id.* at 916.

72. *Id.* at 915.

73. Galloway, *supra* note 10, at 948.

74. 516 F.2d 594 (D.C. Cir. 1975).

75. *Id.* at 614.

purpose of national security, a plurality of the court concluded that "absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional."[76]

II. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

One decade after the passage of Title III, Congress decided to more closely scrutinize the executive branch's use of warrantless electronic surveillance for the purpose of national security. Regardless of the overwhelming support for a limited foreign intelligence surveillance exception to the Fourth Amendment in several circuit courts of appeal, executive abuses of surveillance tactics, such as Watergate, prompted Congress to consider practical limitations on the scope of wiretapping[77] and ultimately enact FISA.

A. *Evolution and Framework of FISA*

Despite almost fifty years of judicial attention to both the constitutionality of warrantless national security wiretapping and the foreign intelligence surveillance exception to the Fourth Amendment, the resulting standards "remained obscure, ambiguous and inconclusive."[78] In 1976, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities ("Church Committee") determined that the executive branch, including the FBI and the CIA, was consistently abusing the power to conduct warrantless national security surveillance against certain targeted groups, including the Women's Liberation Movement and the anti-war movement.[79] Acting on the Church Committee's recommendations that Congress needed to implement a statutory framework to monitor and control foreign intelligence surveillance, Congress passed the Foreign Intelligence Surveillance Act of 1978.[80]

FISA was enacted to authorize electronic surveillance by the President or Attorney General toward the investigation of foreign

76. *Id.* at 614; *see also* George P. Varghese, Comment, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385, 396 (2003).

77. *See* Cinquegrana, *supra* note 29, at 806 (citing FINAL REPORT OF THE SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, FINAL REPORT, BOOK II, S. REP. NO. 94-755 (1976)) [hereinafter Church Committee Report].

78. Cinquegrana, *supra* note 29, at 806.

79. *See* Varghese, *supra* note 76, at 397.

80. *See* Church Committee Report, *supra* note 77, at 299–302, *cited in* Cinquegrana, *supra* note 29, at 807.

powers or agents of foreign powers, which includes terrorist organizations, for the purpose of acquiring foreign intelligence information.[81] Such surveillance is limited to the gathering of foreign intelligence information, which is "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against" the following actions by a foreign power or agent of a foreign power: (a) actual or potential attack, (b) international terrorism, or (c) clandestine intelligence activities.[82]

In an effort to provide a modicum of judicial review with respect to foreign intelligence surveillance, Congress established the Foreign Intelligence Surveillance Court ("FISC"), comprised of eleven district court judges appointed by the Chief Justice of the Supreme Court.[83] To attain a FISA court order to implement electronic surveillance against a foreign power or agent, federal officers must apply for an order approving the wiretapping or search and seizure of a tangible object and must include a certification from the Attorney General that "the purpose of the surveillance is to obtain foreign intelligence information."[84] A FISA court order will be issued if a FISC judge finds that there is "probable cause to believe that the target is a foreign power or an agent of a foreign power and that she is using, or about to use, the facilities targeted by the surveillance."[85] In addition, FISA mandates that the information gathered during the surveillance be used for law enforcement purposes only with authorization from the Attorney General and advance notification to the defendant.[86] Defendants may challenge a FISA order only on the grounds that the information was unlawfully obtained or that

81. *See* 50 U.S.C. §§ 1801–1802 (2000). An agent of a foreign power is defined as a non-United States citizen acting on behalf of a foreign power within the borders of the United States. *Id.* § 1801(b)(1)(A). Under § 1801, Congress established a higher standard for targeted United States citizens, requiring that a United States citizen "knowingly engages in clandestine intelligence" activities before surveillance may be authorized. *Id.* § 1801(b)(2)(A); *see also id.* § 1801(i).

82. *Id.* § 1801(e)(1)(a)–(c).

83. *Id.* § 1803(a). The original FISA mandated the appointment of seven district court judges, but this number was increased to eleven by the Patriot Act. *See* Patriot Act § 208.

84. 50 U.S.C. § 1804(a)(7)(B) (2000). This statute was later amended to change "the purpose" to "a significant purpose." *See* Patriot Act § 218. Additionally, section 215 of the Patriot Act states that officials "may make an application for an order requiring the production of any tangible things . . . for an investigation to protect against international terrorism or clandestine intelligence activities . . . ." Patriot Act § 215.

85. Varghese, *supra* note 76, at 400.

86. 50 U.S.C. § 1806(b)–(c) (2000).

the information acquired surpassed the grant of authority in the FISA order.[87] Such challenges arose often in district courts and circuit courts of appeals nationwide shortly after the passage of FISA.

B. *Constitutionality of FISA and the Primary Purpose Standard for Foreign Intelligence Surveillance*

Between the passage of the original FISA and Patriot Act amendments, FISA was challenged several times on the grounds that its reduced probable cause standard violated the Warrant Clause of the Fourth Amendment. However, the legislative history indicates that FISA was never intended to satisfy the traditional requirements of the Warrant Clause. FISA was enacted to obtain foreign intelligence information, which is vital to national security, an interpretation that was reaffirmed by most circuit courts in the manner of *Truong* and *Butenko*.[88]

In *United States v. Duggan*,[89] the Second Circuit heard an appeal from defendants convicted of conspiracy to smuggle weapons to the Irish Republican Army. The defendants challenged the government's use of foreign intelligence surveillance obtained pursuant to a FISA court order to convict the defendants at trial. *Duggan* confirmed the primary purpose standard stated in *Truong* and asserted that "the procedures fashioned in FISA [are] a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information."[90]

Furthermore, in *United States v. Pelton*,[91] the Fourth Circuit determined that FISA surveillance of a defendant convicted of espionage and conspiracy to commit espionage by transmitting National Security Agency information to the Soviet Union was constitutional under the Fourth Amendment. The *Pelton* court recognized that the surveillance fulfilled the primary purpose standard and stated that "FISA's numerous safeguards provide sufficient protection for the rights guaranteed by the Fourth Amendment within the context of foreign intelligence activities."[92]

87. *See id.* § 1806(e).
88. *See* Varghese, *supra* note 76, at 402–03.
89. 743 F.2d 59 (2d Cir. 1984).
90. *Id.* at 73.
91. 835 F.2d 1067 (4th Cir. 1987).
92. *Id.* at 1075.

However, the Ninth Circuit refused to explicitly affirm the primary purpose test in *United States v. Sarkissian*.[93] The *Sarkissian* court posited that the distinction between foreign intelligence surveillance and criminal investigations is almost immaterial and "passed on the question of whether *Truong* is the constitutional standard in a criminal prosecution."[94] The court refused to "draw too fine a distinction between criminal and intelligence investigations" because acts of international terrorism ultimately entail criminal investigations because terrorism is also a criminal offense.[95]

The conflict among circuit courts regarding whether the *Truong* test should apply to FISA court orders was temporarily resolved when former Attorney General Janet Reno formally adopted the primary purpose standard for contact between the FBI and the Office of Intelligence Policy and Review ("OIPR"). Attorney General Reno "designed new minimization procedures in 1995 that had the practical effect of preventing criminal investigators from exerting any influence on FISA investigations."[96] Thus, the *Truong* primary purpose standard was effectively implemented as the guiding line between law enforcement and foreign intelligence surveillance, but the failure of the Supreme Court to decisively address this question led to the legislative alteration of this standard after the terrorist attacks of September 11, 2001.

III. FISA AND THE IMPACT OF THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, ON FOREIGN INTELLIGENCE SURVEILLANCE FOR NATIONAL SECURITY PURPOSES

In response to September 11th, legislators and administrators immediately began drafting comprehensive legislation to address the inadequacies and inefficiencies of United States law enforcement with respect to terrorism detection and prevention. The Patriot Act addressed several areas of the law but focused intensely on the government's foreign intelligence surveillance capabilities. It became clear that the current state of national security investigations was woefully under-equipped to deal with the types of terrorist threats and attacks that materialized on September 11th. For example, it is possible that had the barriers of

93. 841 F.2d 959 (9th Cir. 1988).

94. Varghese, *supra* note 76, at 405.

95. *Sarkissian*, 841 F.2d at 965.

96. John E. Branch III, *Statutory Misinterpretation: The Foreign Intelligence Court of Review's Interpretation of the "Significant Purpose" Requirement of the Foreign Intelligence Surveillance Act*, 81 N.C. L. REV. 2075, 2083 (2003).

the *Truong* primary purpose test not been implemented in the Attorney General procedural framework, FBI law enforcement could have easily obtained a FISA court order to search the computer of Zacarias Moussaoui, the so-called "twentieth hijacker."[97] Special Agent Coleen Rowley's memo to FBI Director Robert Mueller revealed that law enforcement's ability to gain FISA search warrants for foreign intelligence purposes had been frustrated by the *Truong* test, and permission to search Moussaoui's computer could possibly have prevented the September 11th attacks.[98]

A. *The Terrorist Attacks of September 11, 2001, and the 9/11 Commission*

On September 11, 2001, American Airlines Flight 11 crashed into the South Tower of the World Trade Center in New York City at approximately 8:45 in the morning.[99] Flabbergasted Americans across the country watched live television coverage of the event and remained optimistic that the airplane's collision with the World Trade Center was an accident.[100] These hopes were dashed at 9:05 in the morning, as United Airlines Flight 175 slammed into the North Tower of the New York World Trade Center.[101] Forty minutes later, American Airlines Flight 77 hit the Pentagon in Washington, D.C., and at 10:15 in the morning, United Airlines Flight 93, believed to be aimed at the White House, crashed in a field outside of Pittsburgh, Pennsylvania.[102] And only twenty minutes later, the two World Trade Center Tow-

---

97. *See* Varghese, *supra* note 76, at 408–09.

98. *See Coleen Rowley's Memo to FBI Director Robert Mueller: An Edited Version of the Agent's 13-Page Letter*, TIME ONLINE EDITION, May 21, 2002, *at* http://www.time.com/time/nation/article/0,8599,249997,00.html (on file with the Notre Dame Journal of Law, Ethics & Public Policy) [hereinafter Rowley Memo]. Agent Rowley stated:

> The fact is that key [FBI Headquarters] personnel whose job it was to assist and coordinate with field division agents on terrorism investigations and the obtaining and use of FISA searches . . . continued to, almost inexplicably, throw up roadblocks and undermine Minneapolis' by-now desperate attempts to obtain a FISA search warrant . . . .

Id.

99. *See* Galloway, *supra* note 10, at 922 (citing *America Attacked: World Trade Center, Large Part of Pentagon Destroyed in Terrorist Attack*, *at* http://usgovinfo.about.com/library/blattack0911.htm (last visited Mar. 1, 2005) (on file with the Notre Dame Journal of Law, Ethics & Public Policy) [hereinafter America Attacked]).

100. *Id.*

101. *See id.*

102. *See id.*

ers and a significant portion of the Pentagon lay in ruins.[103] In less than one hour, nineteen fanatical terrorists, wielding only razors or boxcutters, shattered the naïve American belief that two expansive oceans and top-notch national security made the borders of the United States impervious to international terrorism. The September 11th attacks brought large-scale terrorism, which only seemed to exist in Europe and the Middle East, into the living rooms of millions of Americans for the first time.

All facets of the national government mobilized in response to the September 11th terrorist attacks. Attorney General John Ashcroft conducted a large-scale investigation resulting in the arrest of over six hundred possible suspects or material witnesses, and President George W. Bush commenced diplomatic actions to locate and arrest Usama bin Laden, the terrorist leader of al Qaeda who had taken responsibility for the September 11th attacks.[104] However, the most significant reaction to September 11th was the rapid enactment of the Patriot Act. Attorney General Ashcroft implored Congress to approve the pending legislation quickly, as "the American people do not have the luxury of unlimited time in erecting the necessary defenses to future terrorist acts."[105] As a result, Congress passed the Patriot Act on October 25, 2001, and President Bush signed the legislation into law the following day.[106]

In the few years since the terrorist attacks of September 11th and the passage of the Patriot Act, it has become clear that severe structural deficiencies in the executive branch of the federal government prevented law enforcement and intelligence officials from discovering and preventing the September 11th attacks. According to Attorney General Ashcroft, "law enforcement tools created decades ago were crafted for rotary telephone—not email, the Internet, mobile communications, and voice mail. Every day that passes with outdated statutes and the old rules of engagement—each day that so passes is a day that terrorists have a competitive advantage."[107] Furthermore, there were significant legal and bureaucratic obstacles between the CIA and the FBI

103. *See id.*

104. *See* Galloway, *supra* note 10, at 924.

105. John Ashcroft, Testimony Before the House Committee on the Judiciary (Sept. 24, 2001), *at* http://www.usdoj.gov/ag/testimony/2001/agcrisisremarks9_24.htm (on file with the Notre Dame Journal of Law, Ethics & Public Policy) [hereinafter Ashcroft Testimony].

106. *See generally* Patriot Act.

107. Ashcroft Testimony, *supra* note 105.

which prevented the collecting and sharing of foreign intelligence surveillance between intelligence and law enforcement.[108]

The rigid "wall" that divided federal law enforcement and intelligence agencies arguably is a major reason for the inability of law enforcement to detect and prevent the September 11th terrorist attacks.[109] Two documents—the "Phoenix memo" and the Rowley letter—clearly demonstrate the problems inherent in the pre-September 11th national security surveillance structure. First, FBI Agent Kenneth Williams issued a memorandum on July 10, 2001, from the Phoenix branch of the FBI, urging high-level investigators to monitor the attendance at aviation universities and colleges.[110] The purpose of the Phoenix memorandum was to "advise [the FBI] and New York of the possibility of a coordinated effort by Usama bin Laden to send students to the United States to attend civil aviation universities and colleges."[111] Second, FBI Agent Coleen Rowley sent FBI Director Robert Mueller a letter less than one month before the September 11th attacks. The letter detailed the obstacles that the current structure imposed in acquiring a FISA court order to search Zacarias Moussaoui's computer, a search that may have revealed al Qaeda's terrorist plot with enough notice to thwart the attacks. Specifically, Agent Rowley's May 2002 letter indicated that "key [FBI Headquarters] personnel whose job it was to assist and coordinate with field division agents on terrorism investigations and the obtaining and use of FISA searches . . . continued to, almost inexplicably, throw up roadblocks and undermine Minneapolis' by-now desperate attempts to obtain a FISA search warrant."[112]

The deficiencies in the pre-September 11th surveillance structure that were further exposed by these two "smoking gun" documents prompted a congressional hearing in June 2002, and the establishment of the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission"). On June 6, 2002, FBI Director Mueller testified to the proposed and ongo-

108. Press Release, The White House, National Security Advisor Dr. Condoleeza Rice, Opening Remarks, The National Commission on Terrorist Attacks Upon the United States 8 (Apr. 8, 2004), *available at* http://www.9-11commission.gov/hearings/hearing9/rice_statement.pdf (on file with the Notre Dame Journal of Law, Ethics & Public Policy) [hereinafter Rice Testimony].

109. *See id.*

110. *2001 FBI Memo Warned of Bin Laden Aviation Cadre, at* http://www.thesmokinggun.com/archive/0412042phoenix1.html (last visited Mar. 1, 2005) (on file with the Notre Dame Journal of Law, Ethics & Public Policy) [hereinafter Phoenix Memo].

111. *Id.*

112. Rowley Memo, *supra* note 98.

ing changes to the structure of law enforcement, including the fact that "the FBI's shift towards terrorism prevention necessitates the building of a national level expertise and body of knowledge . . . that can be readily shared with our Intelligence Community and law enforcement partners."[113]

President Bush created the 9/11 Commission in late 2002, a few months after the Judiciary Committee's June 2002 hearing on counterterrorism. The purpose of the 9/11 Commission was to "prepare a full and complete account of the circumstances surrounding the September 11, 2001, terrorist attacks, including preparedness for and the immediate response to the attacks."[114] The 9/11 Commission, which published *The 9/11 Commission Report* ("*Commission Report*") on July 22, 2004, heard testimony from many high-level intelligence officials in the Bush administration, including Dr. Condoleezza Rice, the National Security Advisor. The 9/11 Commission issued a comprehensive report detailing the findings on the current state of foreign intelligence surveillance.[115] In *Staff Statement No. 9*, the 9/11 Commission reported that the "wall" between intelligence and law enforcement "caused agents to be less aggressive than they might otherwise have been in pursuing [FISA] surveillance powers in counterterrorism investigations."[116] *Staff Statement No. 12* discusses the implementation of changes to foreign intelligence surveillance after the passage of the Patriot Act and indicates that the removal of the "wall" has facilitated the acquisition of FISA court orders to conduct national security surveillance of foreign powers and agents of foreign powers, but law enforcement and intelligence organizations are still striving for greater fluidity and

113. Robert S. Mueller III, Testimony of the Honorable Robert S. Mueller III Before the Oversight Hearing on Counterterrorism (June 6, 2002), *available at* http://judiciary.senate.gov/testimony.cfm?id=279&wit_id=608 (on file with the Notre Dame Journal of Law, Ethics & Public Policy) [hereinafter Mueller Testimony].

114. Nat'l Comm'n on Terrorist Attacks upon the U.S., *National Commission on Terrorist Attacks Upon the United States*, *at* http://www.9-11commission.gov/.

115. *See generally* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT (2004), *available at* http://www.9-11commission.gov/report/index.htm (on file with the Notre Dame Journal of Law, Ethics & Public Policy) [hereinafter 9/11 COMMISSION REPORT].

116. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., STAFF STATEMENT NO. 9: LAW ENFORCEMENT, COUNTERTERRORISM, AND INTELLIGENCE COLLECTION IN THE UNITED STATES PRIOR TO 9/11, at 7 (2004), *available at* http://www.9-11commission.gov/staff_statements/staff_statement_9.pdf (on file with the Notre Dame Journal of Law, Ethics & Public Policy).

seamlessness with respect to foreign intelligence surveillance.[117] Dr. Condoleezza Rice's statements to the 9/11 Commission affirm the findings of the staff reports and illustrate an important point in assessing the Patriot Act amendments to FISA: "President Bush [has] . . . broken down the bureaucratic walls and legal barriers that prevented the sharing of vital threat information . . . in a way that is consistent with protecting America's cherished civil liberties and with preserving our character as a free and open society."[118]

Ultimately, with respect to the sharing of intelligence information between law enforcement and intelligence agencies, the 9/11 Commission concluded that Reno's 1995 procedures had been misinterpreted and misapplied, resulting in a great deal of confusion with respect to the amount and what type of information could be freely shared between these groups.[119] Without these impediments, the 9/11 Commission indicated that the Phoenix Memo would likely have been distributed to the appropriate agencies in a timely fashion, and Moussaoui and his computer may have been more thoroughly investigated, possibly exposing the September 11th terrorist plot before its execution.[120] According to the *Commission Report*, "[T]hese individual cases did not become national priorities," and there is "little evidence that the progress of the [9/11 terrorist] plot was disturbed by any government action."[121] Thus, the Commission concluded that the "wall" between law enforcement and intelligence thor-

117. *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., STAFF STATEMENT NO. 12: REFORMING LAW ENFORCEMENT, COUNTERTERRORISM, AND INTELLIGENCE COLLECTION IN THE UNITED STATES 7–8 (2004), *available at* http://www.9-11commission.gov/staff_statements/staff_statement_12.pdf (on file with the Notre Dame Journal of Law, Ethics & Public Policy).

118. Rice Testimony, *supra* note 108, at 9.

119. *See* 9/11 COMMISSION REPORT, *supra* note 115, at 78–79, 271. The 9/11 Commission determined that several factors contributed to the establishment of the "wall" between law enforcement and intelligence. While discussing these factors goes beyond the scope of this article, the list of factors includes: (1) the Office of Intelligence Policy and Review assumed the role of conduit of information to the Criminal Division of the FBI, even though Reno's procedures did not include such a provision; (2) the prohibition of sharing intelligence information between FBI agents and criminal prosecutors, which morphed into an artificial barrier among FBI agents; (3) the misconception that FBI agents were prevented from sharing intelligence information with criminal prosecutors, even if FISA had not been invoked; (4) executive orders restricting the flow of this information; and (5) the implementation by some agencies, including the NSA, of requiring permission before sharing intelligence information with criminal prosecutors. *See id.* at 79–80.

120. *See id.* at 272, 276.

121. *Id.* at 277.

oughly hindered American counterterrorism investigation in 2001.

B. *The Patriot Act Amendments to FISA*

While staff statements, Dr. Rice's testimony, and the *Commission Report* itself indicate a general problem with the traditional structure of FISA prior to the September 11th terrorist attacks and comment that the Patriot Act amendments are a vast improvement to the prior regime, it is necessary to examine the specific provisions in greater detail. The most significant portion of the Patriot Act affected FISA and the *Truong* primary purpose standard. As stated in Part II.A, the original language of FISA required that the Attorney General may authorize foreign intelligence surveillance if "the purpose" of the investigation was to gather foreign intelligence information, a requirement that evolved into "the primary purpose" based on the jurisprudence of several circuit courts of appeal.[122] However, section 218 of the Patriot Act changed section 1804(a)(7)(b) to require a designated member of the executive branch to certify that "a significant purpose of the surveillance is to obtain foreign intelligence information."[123] The Act amended FISA so that "intelligence officials may coordinate efforts with law enforcement officials to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities without undermining the required certification of the 'significant purpose' of FISA orders."[124] Approximately four months after the passage of the Patriot Act, Attorney General John Ashcroft executed these amendments by creating a set of Department of Justice ("DOJ") policies to govern the exchange of information between the FBI and the OIPR.[125] Thus, the Patriot Act and its subsequent incorporation into Department of Justice policy effectively removed the wall that Attorney General Reno had erected between criminal investigations and foreign intelligence surveillance.

---

122. *See supra* Part II.A.

123. Patriot Act § 218.

124. Michael J. Bulzomi, *Foreign Intelligence Surveillance Act*, L. ENFORCEMENT BULL., June 2003, at 25, 28, *available at* http://www.fbi.gov/publications/leb/2003/june03leb.pdf (on file with the Notre Dame Journal of Law, Ethics & Public Policy).

125. *Id.*

C. *Judicial Opinions Regarding the Constitutionality of FISA and the "Significant Purpose" Standard as Amended by the Patriot Act*

After Attorney General Ashcroft adopted these new information-sharing policies, the government made a motion to the Foreign Intelligence Surveillance Court ("FISC") on May 17, 2002, to "vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including this Court's adoption of the Attorney General's July 1995 intelligence sharing procedures . . . ."[126] The FISC granted the DOJ's motion, but not without making substantial modifications to parts of the proposed minimization procedures, which included preserving the "wall" between law enforcement and foreign intelligence surveillance and maintaining the policies put in place in 1995 by former Attorney General Reno.[127] According to the FISC, the proposed DOJ procedures did not adequately safeguard civil liberties, and it was concerned that "if criminal prosecutors direct both the intelligence and criminal investigations, or a single investigation having combined interests, *coordination becomes subordination* of both investigations or interests to law enforcement objectives."[128]

On appeal by the DOJ, the Foreign Intelligence Surveillance Court of Review ("Court of Review"), in its first opinion since its creation in 1978, reversed and remanded the ruling of the FISC. The Court of Review held that "FISA, as amended by the Patriot Act, supports the government's position, and that the restrictions imposed by the FISA court are not required by FISA or the Constitution."[129] The Court of Review determined that FISA did not require the government to demonstrate that criminal prosecution was not the primary purpose of the foreign intelligence surveillance, which essentially abandons the *Truong* test, and did not prohibit the DOJ from utilizing foreign intelligence information in criminal proceedings where a significant purpose of the FISA surveillance was for the purpose of gathering national security information.[130] Furthermore, the Court of Review determined that the Patriot Act amendments to FISA, including the "significant purpose" test, did not violate the Fourth Amendment. The

126. *In re* All Matters Submitted to the Foreign Int. Surv. Court, 218 F. Supp. 2d 611, 613 (Foreign Int. Surv. Ct. Rev. 2002).

127. *See id.* at 625–26.

128. *Id.* at 623–24.

129. *In re* Sealed Case No. 02-001, 310 F.3d 717, 719–20 (Foreign Int. Surv. Ct. Rev. 2002) (citation omitted).

130. *Id.* at 727. "In sum, we think that the FISA as passed by Congress in 1978 clearly did *not* preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution." *Id.*

Court of Review determined that the circumstances surrounding national security crimes necessarily dictate a lower standard for FISA authorization than criminal search warrants, and the Patriot Act's "significant purpose" standard is reasonable under the Fourth Amendment.[131]

IV. CONSTITUTIONALITY OF FISA AS AMENDED BY § 218 OF THE PATRIOT ACT

The Supreme Court has yet to determine whether FISA, as amended by section 218 of the Patriot Act, is constitutional. Without a Supreme Court case directly on point, the federal circuit courts of appeal are free to independently draw their own conclusions as to whether this version of FISA satisfies the requirements of the Fourth Amendment. While the decision of the Court of Review binds only the FISC and is not controlling authority in any other federal court, *In re Sealed Case* provides significant guidance to federal district courts and circuit courts of appeal in determining the constitutionality of FISA. There are several compelling arguments—many of which are explained in the opinion of the Court of Review—that illustrate FISA's ability to comply with both independent elements of the Fourth Amendment. First, FISA and the Patriot Act amendments do not violate the Warrant Clause of the Fourth Amendment. Many courts view FISA court orders as search warrants, and FISA technically satisfies the elements of a valid warrant cataloged in *Dalia v. United States*.[132] Second, if FISA court orders are indeed not traditional search warrants, FISA certainly fulfills the Fourth Amendment's Reasonableness Clause. In the wake of September 11th, the government's compelling interest in issues of national security, combined with the President's inherent authority in the area of foreign affairs, contributes to the constitutionality of FISA and the "significant purpose" test of section 218 of the Patriot Act.

A. *FISA Does Not Violate the Warrant Clause of the Fourth Amendment*

The Warrant Clause of the Fourth Amendment states, "no warrants shall issue, but upon probable cause, supported by oath

131. ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND RECENT JUDICIAL DECISIONS 80 (Cong. Research Serv. Report, No. RL30465, 2003), *available at* http://www.fas.org/irp/crs/RL30465.pdf (on file with the Notre Dame Journal of Law, Ethics & Public Policy).

132. *See* Dalia v. United States, 441 U.S. 238, 255 (1979).

or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[133] No court has definitively determined that FISA court orders are the types of search warrants envisioned by the Fourth Amendment, and, in fact, the Court of Review declined to resolve this issue in *In re Sealed Case.*[134] However, there is some judicial support for the contention that FISA court orders qualify as traditional search warrants.[135] In order for FISA court orders to fulfill the Warrant Clause of the Fourth Amendment, the FISA orders must satisfy the *Dalia* Court's three requirements for traditional warrants in criminal investigations:

> First, warrants must be issued by neutral, disinterested magistrates. Second, those seeking the warrant must demonstrate to the magistrate their probable cause to believe "the evidence sought will aid in a particular apprehension or conviction" for a particular offense. Finally, "warrants must particularly describe the 'things to be seized,' as well as the place to be searched."[136]

FISA court orders clearly satisfy the first prong of the *Dalia* test for the constitutionality of search warrants. Typical applications for search warrants under Title III for electronic surveillance must "be made in writing upon oath or affirmation to a judge of competent jurisdiction . . . ."[137] Similarly, under section 1803 of FISA, applications for FISA warrants are received and reviewed by the members of the FISC.[138] The Chief Justice of the Supreme Court selects the FISC "from seven of the United States judicial circuits."[139] Several courts unanimously agree that a "FISC judge qualifies as a neutral and detached magistrate and is an Article III judge."[140]

---

133. U.S. CONST. amend. IV.

134. *Sealed Case*, 310 F.3d at 741. The Court of Review stated that "a FISA order may not be a 'warrant' contemplated by the Fourth Amendment" and refused to resolve the issue in the opinion. *Id.*

135. *See* United States v. Cavanagh, 807 F.2d 787, 790 (9th Cir. 1987); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); United States v. Falvey, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982).

136. *Dalia*, 441 U.S. at 255 (citations omitted).

137. 18 U.S.C. § 2518(1) (2000).

138. 50 U.S.C. § 1803(a) (2000).

139. *Id.* § 1803(b).

140. Jessica M. Bungard, *The Fine Line Between Security and Liberty: The "Secret" Court Struggle to Determine the Path of Foreign Intelligence Surveillance in the Wake of September 11th*, U. PITT. J. TECH. L. & POL'Y, Spring 2004, at 30, *available at* http://www.pitt.edu/~sorc/techjournal/articles/ Vol7Bungard.pdf (on file with the Notre Dame Journal of Law, Ethics & Public Policy) (citation omitted).

The third element, which requires that the warrant describe with particularity the objects to be seized and the locations that will be searched, is almost as easily satisfied as the first prong of the *Dalia* test. Section 1804(a) of FISA requires that any federal officer applying for a FISA court order must submit a lengthy and detailed application for electronic surveillance,[141] and these factors clearly fulfill both aspects of the particularity requirement. First, the seized items or objects must be included in the warrant under section 1804(a)(6), which states that each FISA order must include "a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance."[142] Second, the locations that will be "searched" (under surveillance) are listed in the FISA order under section 1804(4)(b), which asserts that the application must include a "statement of the facts and circumstances relied upon by the applicant to justify his belief that each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."[143] These elements are required in every FISA order because the Attorney General must certify that all elements of the FISA application under section 1804(a) have been fulfilled.[144]

Probable cause, the second element of the *Dalia* warrant test, is the most controversial with respect to FISA surveillance. FISA does have a probable cause standard, but it differs from the probable cause standard in Title III. Title III "authorizes electronic surveillance if it determines that 'there is a probable belief that an individual is committing, has committed, or is about to commit' a specified predicate offense."[145] FISA requires a reduced standard of probable cause, which only entails certification that the subject of the electronic surveillance is a foreign power or acting as an agent of a foreign power.[146] However, this difference is not an oversight—the legislative history of FISA indicates that Congress did not intend FISA and Title III to have equivalent probable cause standards. Congress burdened FISA with additional safeguards that it did not impose on Title III, including the inability to use FISA for domestic terrorism pur-

141. 50 U.S.C. § 1804(a) (2000).

142. *Id.* § 1804(a)(6).

143. *Id.* § 1804(a)(4)(2).

144. *Id.* § 1804(a)(1–11).

145. Bungard, *supra* note 140, at 27 (quoting 18 U.S.C. § 2518(3)(a) (2000)).

146. 50 U.S.C. § 1804(a)(4)(A).

poses.[147] And while civil liberties groups have questioned whether FISA's probable cause standard infringes upon individual freedoms, it only applies to *foreign* powers or *agents* of foreign powers, and FISA consistently has been held constitutional by several district courts and circuit courts of appeal since its enactment in 1978.[148]

B. *FISA Does Not Violate the Reasonableness Clause of the Fourth Amendment*

In order for law enforcement officials to conduct warrantless electronic surveillance pursuant to either of these exceptions to the Fourth Amendment, the wiretapping must satisfy the Reasonableness Clause of the Fourth Amendment. The Reasonableness Clause of the Fourth Amendment states that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[149] In interpreting this clause, the Supreme Court has consistently held that the reasonableness of the search is determined by "balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[150]

Assuming that FISA court orders do not satisfy the traditional warrant requirement of the Fourth Amendment as interpreted by the *Dalia* Court,[151] electronic surveillance for the purpose of national security requires a valid exception to the Fourth Amendment that excuses the search's lack of prior judicial review. Two compelling justifications exist to support the constitutionality of FISA as amended by the Patriot Act. First, FISA qualifies under the "special needs" exception to the Fourth Amendment, which allows "reasonable, warrantless searches for

147. *See In re* Sealed Case No. 02-001, 310 F.3d 717, 739 (Foreign Int. Surv. Ct. Rev. 2002); *see also* Bungard, *supra* note 140, at 31 ("The fact that FISA provides replacements for Title III procedures make it seem equally safeguarded against infringement upon liberties.").

148. United States v. Cavanagh, 807 F.2d 787, 792 (9th Cir. 1987); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); United States v. Falvey, 540 F. Supp. 1306, 1316 (E.D.N.Y. 1982).

149. U.S. CONST. amend. IV.

150. Delaware v. Prouse, 440 U.S. 648, 654 (1979); *see also* Tennessee v. Garner, 471 U.S. 1, 8 (1985). In *Garner*, the Court looks at all surrounding circumstances to determine whether the government's interests outweigh the "nature and quality of the intrusion on the individual's Fourth Amendment interests." *Id.* (quoting United States v. Place, 462 U.S. 696, 703 (1983)).

151. *See* Bungard, *supra* note 140, at 31.

government needs that go beyond regular law enforcement."[152] Second, the government's compelling interest in preserving the national security bolsters the argument in favor of adopting a national security exception to the Fourth Amendment that would encompass FISA as amended by the Patriot Act.

1. FISA Qualifies Under the "Special Needs" Exception to the Fourth Amendment

A "special needs" exception to the Fourth Amendment has long been recognized by the Supreme Court. In *New Jersey v. T.L.O.*,[153] Justice Blackmun stated in his concurrence that "[o]nly in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers."[154] Justice Blackmun's concurrence with respect to the special needs doctrine was subsequently accepted by a majority of the Court in *Griffin v. Wisconsin*.[155] The special needs exception has been applied in several contexts, including alcohol and drug testing for railway employees,[156] drug testing for United States Customs Service employees,[157] drunk driving checkpoints,[158] and drug testing for public officials.[159]

Using the *Griffin* balancing test, FISA and its "significant purpose" standard can be justified under the special needs exception to the Fourth Amendment. Admittedly, the "significant purpose" test outlined in section 218 of the Patriot Act authorizes law enforcement and foreign intelligence agencies to more freely share information acquired through FISA surveillance and allows FISA wiretapping when criminal prosecution is a major goal of the operation. However, the "significant purpose" standard is

152. Testimony of John Yoo Before Hearing on Securing Freedom and the Nation Collecting Intelligence under the Law, Constitutional and Public Policy Considerations (Oct. 30, 2003), *at* http://www.fas.org/irp/congress/2003_hr/103003yoo.pdf (on file with the Notre Dame Journal of Law, Ethics & Public Policy).

153. 469 U.S. 325 (1985).

154. *Id.* at 351.

155. 483 U.S. 868, 873 (1987). Specifically, *Griffin* recognized the special needs exception to the Fourth Amendment when law enforcement officials require such searches for reasons beyond the normal needs of law enforcement. *Id.*

156. Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665–66 (1989).

157. Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 619 (1989).

158. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 444–50 (1990).

159. Chandler v. Miller, 520 U.S. 305, 313 (1997).

justified under the special needs doctrine because, in the wake of September 11th, the detection and prevention of terrorist attacks is the type of emergency hazard that far surpasses the "normal" need for law enforcement. The traditional "wall" between law enforcement and foreign intelligence surveillance handicapped the government's investigations of terrorist activity, and the government's interest in maintaining this reduced standard outweighs individual civil liberties in light of the possibility of future attacks of a greater scale than September 11th.

Opponents of the Patriot Act amendment argue that the "significant purpose" standard allows the government to circumvent Title III's warrant requirement and masks criminal prosecutions as FISA electronic surveillance.[160] However, the Court of Review acknowledged that "FISA's general programmatic purpose, to protect our nation against terrorists and espionage threats directed by foreign powers, has from its outset been distinguishable from 'ordinary crime control.'"[161] In *City of Indianapolis v. Edmond*,[162] the Court held that a highway checkpoint was erected for the primary purpose of ordinary criminal law enforcement and did not meet the requirements of the special needs doctrine.[163] However, the Court stated that "the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack."[164] The *Edmond* decision indicates that the Court will consider the nature and gravity of the threat involved when applying the special needs doctrine, and the prevention of terrorism likely justifies the "significant purpose" test under this exception.

2. FISA Qualifies Under a Limited Foreign Intelligence Exception to the Fourth Amendment

Although FISA's "significant purpose" standard finds adequate support under the special needs exception, the more compelling argument in favor of its constitutionality is that FISA would satisfy the requirements of a limited foreign intelligence exception to the Fourth Amendment. While the Supreme Court has not addressed this question, there is a significant body of jurisprudence among federal district courts and circuit courts of

160. *See, e.g.*, Stephanie Kornblum, *Winning the Battle While Losing the War: Ramifications of the Foreign Intelligence Surveillance Court of Review's First Decision*, 27 SEATTLE U. L. REV. 623, 627 (2003).

161. *In re* Sealed Case No. 02-001, 310 F.3d 717, 746 (Foreign Int. Surv. Ct. Rev. 2002).

162. 531 U.S. 32 (2000).

163. *Id.* at 41–42.

164. *Id.* at 44.

appeal indicating a growing support for such a national security doctrine.[165] The existence of a foreign intelligence exception requirement to the Fourth Amendment would nullify opponents' arguments that question the constitutionality of FISA as amended by the Patriot Act. Since any searches and seizures potentially justified under a foreign intelligence exception must still satisfy the Reasonableness Clause of the Fourth Amendment, a simple balancing test between the governmental interest in national security and foreign affairs and potential infringement upon individual civil liberties must be employed.[166] Three arguments highlight the reasonableness of FISA and the "significant purpose" test under the Fourth Amendment. Judicial deference to the President and executive department in the area of foreign affairs, the increased threat to national security from extremist terrorist organizations in the wake of September 11th, and FISA's similarity with Title III, all support the contention that FISA's "significant purpose" test in section 218 of the Patriot Act satisfies the Reasonableness Clause of the Fourth Amendment.

As discussed in Part I, there is considerable case law in the lower federal courts supporting a limited foreign intelligence exception to the Fourth Amendment. Several circuit courts, namely the Third, Fourth, Fifth, and Ninth Circuits, have justified warrantless electronic surveillance for national security purposes by adopting a foreign intelligence exception to the Fourth Amendment.[167] In determining whether to adopt such a doctrine, these circuit courts depended heavily on the inherent powers of the President with respect to international relations, as discussed *infra*. The *Brown* Court, for example, holds that the President's inherent authority in national security issues authorizes the President to obtain foreign intelligence without a traditional criminal warrant.[168]

The difficulty with these circuit court decisions, as well as those that have held the original FISA constitutional under the Fourth Amendment, is that many of these rulings utilize the "primary purpose" test, which posits that the primary purpose of electronic wiretapping must be the acquisition of foreign intelligence information for reasons of national security. These deci-

165. *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 916 (4th Cir. 1980); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); United States v. Butenko, 494 F.2d 593, 608 (3d Cir. 1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973).

166. *See* United States v. United States Dist. Court (Keith), 407 U.S. 297, 322–23 (1972).

167. *See* cases cited *supra* note 165.

168. *See Brown*, 484 F.2d at 426.

sions directly contradict the "significant purpose" standard in section 218 of the Patriot Act. The decision in *In re Sealed Case* dispenses with this standard because the "primary purpose" test emerged from lower court interpretations, and finds no textual grounding in the original FISA. The Court of Review disapproved of these decisions "for relying too heavily upon the precedent in *Truong* and not upon the plain, unadorned language and the plain intent of the original language of [the statute]."[169] The Court of Review seemed to prefer the viewpoint of the *Sarkissian* court. In *Sarkissian*, the Ninth Circuit noted that the distinction between acquiring intelligence information for national security purposes and criminal prosecution purposes is virtually immaterial.[170] The fact that information acquired through national security surveillance may ultimately lead to criminal prosecutions is not problematic because the initial purpose of gathering such information is to combat international terrorism, and the fruits of these investigations can constitutionally be used in later criminal prosecutions. Thus, the reasonableness of the "significant purpose" test under FISA is buttressed by the significant case law articulating a limited foreign intelligence exception to the Fourth Amendment, and the fact that some of these decisions interpret a "primary purpose" test for foreign intelligence does not detract from the newly amended statute's reasonableness.

While the Court of Review used in part a statutory interpretation argument to justify the legitimacy of the "significant purpose" of the Patriot Act, additional constitutional and policy arguments further strengthen this argument. First, it is well-settled that the executive branch, primarily the President, has both the authority and duty to safeguard the Constitution. The Presidential Oath in Article II of the Constitution requires the President to "preserve, protect and defend the Constitution of the United States."[171] The jurisprudence of the Supreme Court regarding the President's inherent authority to unilaterally conduct matters of foreign affairs is substantial. In *United States v. Curtiss-Wright*,[172] the Supreme Court discussed the "very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations."[173] Specifically, the *Curtiss-Wright* Court indicated that the President is far more knowledgeable than Congress with respect to the President's greater opportunity to assess the issues of national

169. *Bungard, supra* note 140, at 18.
170. Sarkissian v. United States, 841 F.2d 959, 965 (9th Cir. 1988).
171. U.S. CONST. art. II, § 1, cl. 8.
172. 299 U.S. 304 (1936).
173. *Id.* at 320.

security in a particular foreign country.[174] The Court further limited foreign affairs to the discretion of the executive branch in *Chicago & Southern Air Lines v. Waterman S.S. Corporation*,[175] which held that the judiciary should not interfere with matters of national security.[176] According to the Court, foreign policy is of a political nature, and related decisions are "delicate, complex, and involve large elements of prophecy."[177] Several years after the *Waterman* decision, the Court in *Keith* interpreted Article II to mean that "implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means."[178]

Not only does the President have a general plenary power in the areas of national security and foreign affairs, but the executive branch has specific authority over the collection of foreign intelligence information.[179] The Supreme Court has not limited its wiretapping capabilities to electronic surveillance for the "primary purpose" of collecting national security information, which implies that surveillance for the "significant purpose" of collecting foreign intelligence information would not subvert the intention of the judiciary. Thus, it is reasonable for the Attorney General to implement a standard that allows simultaneous criminal prosecutions and foreign intelligence surveillance against a legitimate target with overlap between law enforcement and intelligence officials.

Second, public policy reasons dictate that the governmental need in protecting the United States from further terrorist attacks of September 11th proportions far outweighs exaggerated concerns for the curtailment of individual privacy rights. According to *Time* magazine, "The amorphous nature of [the terrorist] plotters' network enabled it to operate under the noses of intelligence and police forces."[180] The recent terrorist bombing in Madrid, Spain, illustrates the ease with which terrorist organizations operate in and around target countries, and the problems that law enforcement officials face when trying to quell such attacks. The *New York Times* reported that "agents tracking [terrorists] . . . are constrained by jurisdictional and bureaucratic boundaries. Intelligence is far too infrequently shared . . . often

174. *Id.*
175. 333 U.S. 103 (1948).
176. *Id.* at 111.
177. *Id.*
178. United States v. United States Dist. Court (Keith), 407 U.S. 297, 308 (1972).
179. Totten v. United States, 92 U.S. 105, 106 (1875).
180. Johanna McGeary, *Who's the Enemy Now*, TIME, Mar. 29, 2004, at 29.

leaving information about dangerous militants woefully incomplete."[181] This intelligence problem is not confined to Europe, as September 11th demonstrated how al Qaeda's efforts were facilitated by the informational breakdown between law enforcement and intelligence officials. Thus, the difficulties with infiltrating a terrorist organization indicate that, currently, the only practicable alternative is to condone widespread electronic surveillance for the "significant purpose" of obtaining foreign intelligence, which may contribute later to criminal prosecutions of terrorists.

Finally, because FISA, as amended by the Patriot Act, provides several provisions that protect individual rights to a greater extent than Title III and its traditional warrant requirements for criminal investigations, civil liberties groups cannot successfully argue that individual liberties outweigh the compelling governmental need for increased surveillance powers and communication between law enforcement and intelligence officials. FISA and Title III share several significant protective provisions, but FISA provides additional safeguards in certain areas that far surpass its Title III counterpart. First, both Title III and FISA appear to satisfy the requirements for a warrant, as discussed in Part IV.A. Both statutes demand prior judicial authorization for electronic surveillance, although Title III requires a traditional search warrant.[182] In addition, FISA and Title III contain probable cause requirements, but FISA's probable cause standard does not mandate certification that the target has committed or is committing a crime.[183] Probable cause under FISA pertains only to whether the target is a foreign power or agent of a foreign power.[184]

While FISA facially appears to allow more encroachment on civil liberties than Title III, FISA implements several measures to further protect the public from unconstitutional searches and seizures under the Fourth Amendment with respect to national security surveillance. While the probable cause standard under FISA is demonstrably lower, it is virtually impossible for law enforcement officials to completely circumvent Title III in conducting electronic surveillance with crimes that have no discernable nexus to national security concerns. For example, "FISA surveillance would also not be authorized against a target

181. Tim Golden et al., *As Europe Hunts for Terrorists, the Hunted Press Advantages*, N.Y. TIMES, Mar. 22, 2004, at A1.

182. *See In re* Sealed Case No. 02-001, 310 F.3d 717, 738 (Foreign Int. Surv. Ct. Rev. 2002).

183. *Id.*

184. *Id.*

engaged in purely domestic terrorism because the government would not be able to show that the target is acting for or on behalf of a foreign power."[185]

Ultimately, the Court of Review posited that if FISA does "not meet the minimum Fourth Amendment warrant standards, [it] certainly comes close."[186] Thus, the fact that FISA closely mirrors Title III in many respects and provides additional safeguards for individual liberties strongly contributes to the reasonableness of FISA as amended by the Patriot Act. The combination of the government's compelling interests in a pervasive foreign intelligence surveillance statute to adequately combat foreign terrorist threats and a reduced concern with encroachment on civil liberties suggests that section 218 of the Patriot Act clearly satisfies the Reasonableness Clause of the Fourth Amendment.

CONCLUSION

The terrorist attacks of September 11, 2001, dramatically highlighted the startling inadequacies of prior legislation that had been enacted to address the problems of domestic and international terrorism and underscored the need to re-evaluate this legislation in light of such unprecedented and catastrophic events. The speedy passage of the Patriot Act in October 2001 quickly augmented the sparse arsenal that law enforcement officials maintained to combat terrorism by granting such officials sweeping powers in several areas, which included facilitating law enforcement officials in conducting electronic surveillance for national security purposes. Section 218 of the Patriot Act amended FISA by lowering the required threshold to conduct surveillance against specified targets. While the Attorney General initially had to certify that such national security surveillance was for "the purpose" of obtaining foreign intelligence information, the Patriot Act authorized FISA court orders if a "significant purpose" of the investigation was foreign intelligence surveillance. The mere substitution of a few words buried in the middle of FISA arguably caused more controversy than most other aspects of the Patriot Act. The rallying cry of most civil liberties groups was that FISA as amended would allow law enforcement officials to effortlessly circumvent the traditional warrant requirements of the Fourth Amendment.

However, this analysis is unsupported because FISA and section 218 of the Patriot Act clearly satisfy both the Warrant Clause and the Reasonableness Clause of the Fourth Amendment. Sev-

185. Bungard, *supra* note 140, at 28.
186. *Sealed Case*, 310 F.3d at 738.

eral federal courts have held that FISA court orders qualify as warrants, and the elements of the FISA statute indicate that FISA seemingly satisfies the three requirements posited in *Dalia*. First, FISA warrants are granted by neutral Article III magistrates. Second, these court orders contain sufficient particularity with respect to the targeted individual, any targeted facilities, and any facts and circumstances that explain the nexus among the target, the facilities, and the electronic wiretapping. Finally, FISA warrants require a reduced probable cause standard that has consistently been held constitutional.

Furthermore, there are several persuasive reasons that FISA fulfills the Reasonableness Clause of the Fourth Amendment. First, FISA appears to fall under the special needs exception to the Fourth Amendment, which allows law enforcement officials to conduct warrantless searches when emergency situations arise, which would make the warrant requirement cumbersome and detrimental to the specified investigation. Second, the governmental interest in preserving the national security of the United States in the wake of the September 11th terrorist attacks by engaging in foreign intelligence surveillance far outweighs individual fears that civil liberties are being unconstitutionally compromised. The President's inherent authority in the area of foreign affairs indicates that the executive branch has ample power to engage in warrantless foreign surveillance for virtually any purpose that has a significant nexus to gathering foreign intelligence information. This judicial deference to the executive branch with respect to national security has contributed heavily to the development of a limited foreign intelligence exception to the Fourth Amendment in several courts of appeal. Finally, FISA's multiple similarities to Title III and its additional safeguards throughout the statute to prevent encroaching on civil liberties indicate that individual concerns about individual liberties are unfounded. Thus, the balancing test articulated numerous times by the Supreme Court weighs heavily in the government's favor, meaning that FISA as amended by section 218 of the Patriot Act is not unconstitutional under the Fourth Amendment.