COMMENTS

BEYOND "PERSONS, HOUSES, PAPERS, AND EFFECTS": REWRITING THE FOURTH AMENDMENT FOR NATIONAL SECURITY SURVEILLANCE

by
Elizabeth Gillingham Daily[*]

Although the goal of national security surveillance is to protect the nation against terrorist acts such as the September 11, 2001 attacks, the Patriot Act amendments to the Foreign Intelligence Surveillance Act ("FISA") have been interpreted to permit surveillance where the primary purpose of the surveillance is criminal prosecution and not foreign intelligence. FISA surveillance may now be used as a tool for prosecution of any foreign intelligence crime or crime that is inextricably linked with foreign intelligence. It does not require the government to establish any likelihood that evidence of a crime or a threat to national security will be found and places immense power in the hands of law enforcement to intrude on that individual's privacy. This Comment discusses the unique concerns national security surveillance under the Fourth Amendment poses and concludes that additional safeguards are needed to protect the rights of both individuals and the government.

[*] J.D. 2006, Lewis & Clark Law School.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[1]

I. INTRODUCTION

The Fourth Amendment has fifty-four words. Those fifty-four words define the line between legitimate law enforcement practices and inviolable individual privacy. But the line that they define is indistinct. What is an "unreasonable" search or seizure? What is "probable cause"? When does the lack of a warrant render a search unreasonable?

In the realm of national security surveillance conducted by the Executive Branch, the line drawn by the Fourth Amendment is particularly difficult to discern for several reasons. First, the Framers drafted the Fourth Amendment to protect against physical intrusions, such as general warrants and writs of assistance. However, national security surveillance relies on the use of technologically-enhanced methods of surveillance such as wiretaps.[2] While broad in their ability to obtain vital information, these methods of surveillance do not involve physical force or intrusion.

Second, the goal of national security surveillance is to protect the country against grave threats from terrorism rather than the more moderate threat of ordinary crime. The gravity of the threat presented is not mentioned in the Fourth Amendment, but it may play a role in determining the type of search or seizure that would be considered "unreasonable."[3] The September 11 attacks graphically demonstrated the consequences that may result from intelligence failures that put national security at risk. Because of the importance of preventing massive catastrophes, it may be "reasonable" to authorize more serious intrusions into privacy and less restraint on executive conduct when national security is at risk than under circumstances where the consequences of failure are less serious.

This Comment will discuss national security surveillance under the Fourth Amendment from a historical and modern perspective. Part II of the Comment will describe the development of wiretapping as a law enforcement tool, its use in national security matters, and the original application of the Fourth Amendment to electronic surveillance. Part III will track congressional and judicial regulation of national security surveillance from 1967 to 1978. Part IV will discuss the enactment of the Foreign Intelligence Surveillance Act (FISA) and subsequent judicial opinions applying the Fourth Amendment to FISA surveillance. Part V will discuss the Patriot Act and the Foreign Intelligence

---

[1] U.S. CONST. amend. IV.

[2] *See infra* Part III (describing use of wiretapping for national security surveillance).

[3] *See* City of Indianapolis v. Edmond, 531 U.S. 32, 42 (2000) (recognizing that the gravity of the threat involved is not dispositive in determining the means law enforcement may employ to pursue a given purpose).

Surveillance Court of Review's opinion, *In re Sealed Case*.[4] And Section VI will analyze whether *In re Sealed Case* appropriately balanced the Fourth Amendment's protection of individual rights with the government's legitimate need to conduct foreign intelligence surveillance. This section concludes that the *In re Sealed Case* decision violated the Fourth Amendment by expanding FISA surveillance to criminal investigations without placing sufficient checks on executive abuse.

The Comment concludes that national security surveillance presents unique concerns under the Fourth Amendment, and the only guidepost provided by the language of the Constitution itself is "reasonableness." Under this standard, considering the history of executive abuse, additional safeguards are needed to protect both government interests and individual rights.

II. WIRETAPPING UNDER THE FOURTH AMENDMENT

A. Historical Use of Wiretaps by the Government

Wiretapping was invented almost simultaneously with the invention of wire communications in 1844.[5] Wiretaps allow a person to intercept private conversations by placing a listening device on the communication wires. When law enforcement agents turned wiretapping into an investigatory tool at the beginning of the twentieth century, it quickly became invaluable.[6] Wiretaps allowed agents to gain critical information about criminals without the risk of confrontation.[7] More importantly, the technology allowed law enforcement to appear "all-knowing, all-seeing, [and] all-powerful."[8]

In the 1930s, as the country geared up for World War II, the Executive Branch, driven by FBI Director J. Edgar Hoover, began using wiretaps to conduct secret electronic surveillance for national security purposes.[9] President Roosevelt tacitly approved this surveillance in 1940 when he stated that use of electronic surveillance would be proper when it was necessary to gain intelligence in "grave matters involving [the] defense of the nation."[10] Roosevelt cautioned that surveillance should be limited to suspected spies and, wherever possible, should only be used against aliens and not against United States citizens.[11] The Executive Branch claimed that the authority to conduct warrantless surveillance derived from the President's inherent powers in the realm of foreign affairs, but this claim was never decided by the Supreme

---

[4] 310 F.3d 717 (FISA Ct. Rev. 2002).

[5] ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 154 (2000).

[6] *Id*.

[7] *Id*.

[8] *Id*.

[9] *Id*. at 160.

[10] S. REP. NO. 95-604, pt. 1, at 10 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3911.

[11] *Id*.

Court.[12] In later years, the Church Committee, convened to investigate affairs surrounding the Watergate scandal and secret executive surveillance of political enemies, reported that the period between 1936 and 1945 "opened the institutional door to greater excesses in later years."[13]

Over the next several decades, government use of wiretaps quickly expanded.[14] By the 1950s, the FBI authorized itself to use electronic surveillance at its own say-so, as long as the "national interest" required the surveillance.[15] In 1976, the Church Committee determined that every president since Roosevelt asserted and continued to exercise the authority to conduct secret electronic surveillance without attempting to obtain any prior judicial approval.[16]

B. Wiretapping Under the Fourth Amendment: Olmstead *and* Katz

In 1928, the Supreme Court addressed wiretapping. In *Olmstead v. United States*,[17] the Court hewed to a literal interpretation of the Fourth Amendment's text and held that wiretap surveillance does not fall within the scope of the Fourth Amendment.[18] The *Olmstead* opinion, authored for the majority by Chief Justice Taft, reasoned that the scope of the Fourth Amendment could not extend beyond the search and seizure of tangible items, such as the items listed in the text of the amendment itself: persons, houses, papers and effects.[19] Since government agents were able to intercept conversations by wiretap without physically invading the defendant's house, the protections of the Fourth Amendment did not apply to that activity. [20]

In his famous dissent, Justice Brandeis argued that the Court should look beyond the text of the Fourth Amendment and examine its underlying purpose.[21] Brandeis argued that the Fourth Amendment protects against government invasion of individual privacy and creates the "right to be let alone."[22] Thus, the scope of the Fourth Amendment's protection should not be limited to the methods of invasion reviled by the Framers such as writs of assistance and general warrants.[23] The Fourth Amendment's protection must expand to combat the "[s]ubtler and more far-reaching means of invading

---

[12] *Id*. at 9.

[13] SELECT COMM. TO STUDY GOV'TL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, S. REP. NO. 94-755, at 24 (1976) [hereinafter CHURCH COMMITTEE REPORT, BOOK II].

[14] *Id*. at 21.

[15] S. REP. NO. 95-604, pt. 1, at 11.

[16] CHURCH COMMITTEE REPORT, BOOK II, *supra* note 13, at 9.

[17] 277 U.S. 438 (1928).

[18] *Id*. at 466.

[19] *Id*. at 464.

[20] *Id*. at 466.

[21] *Id*. at 472 (Brandeis, J., dissenting).

[22] *Id*. at 478.

[23] *Id*. at 476.

privacy" represented by wiretapping and other developing technologies.[24] Asserting that the Constitution is a living document, Brandeis urged a flexible and purposeful interpretation to cope with the problems of the future: "[A] principle to be vital must be capable of wider application than the mischief which gave it birth."[25]

Despite Brandeis' powerful rhetoric in dissent, the *Olmstead* majority's literal interpretation of the Fourth Amendment remained the prevailing law on government use of wiretaps until 1967 when the Supreme Court decided *Katz v. United States*.[26] In *Katz*, the Court overruled *Olmstead* and held that wiretapping falls within the scope of the Fourth Amendment.[27] The Court rejected the notion that the Fourth Amendment only protects against physical trespass into protected areas.[28] In famous language, Justice Stewart stated in his majority opinion:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[29]

The Court held that wiretaps were sufficiently intrusive to implicate Fourth Amendment protection, meaning a presumption against warrantless surveillance.[30] The court stated that the government's self-imposed limitation on the scope of the surveillance did not render the surveillance "reasonable" under the Fourth Amendment because, "the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer."[31]

The Supreme Court's *Katz* decision placed the President's established practice of conducting warrantless electronic surveillance for the purpose of national security in question for the first time. The decision acknowledged the issue in a footnote, but refused to pass judgment: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment

---

[24] *Id*. at 473. Justice Brandeis anticipated that the government's developing ability to pry into individual lives would not stop with wiretapping: "Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be able to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions." *Id*. at 474. His fears may be partially justified with the development of internet surveillance and infrared search technology.

[25] *Id*. at 472–473 (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

[26] 389 U.S. 347 (1967). In Nardone v. United States, 302 U.S. 379, 381 (1937), the Supreme Court held that evidence obtained by wiretaps may not be used as evidence in court based on the Federal Communications Act of 1934, but it did not hold that the Constitution itself prohibited wiretapping.

[27] 389 U.S. at 353.

[28] *Id*. at 351.

[29] *Id*. (citations omitted).

[30] *Id*. at 356.

[31] *Id*.

in a situation involving the national security is a question not presented by this case."[32]

Justice White, in concurrence, argued that the warrant requirement should not apply to national security surveillance:

> Wiretapping to protect the security of the Nation has been authorized by successive Presidents . . . . We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.[33]

Justice Douglas's concurrence, in contrast, characterized Justice White's opinion as an "unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels 'national security' matters."[34] Justice Douglas argued that the warrant requirement should apply to national security surveillance because the President and the Attorney General hardly qualified as neutral magistrates to ensure the protection of Fourth Amendment rights.[35] Douglas warned that the Judicial Branch must serve as a neutral and disinterested party mediating between the legitimate needs of law enforcement and the individuals targeted by the government for surveillance.[36]

The question that was at issue between Douglas and White—the efficacy of self-imposed regulation and restraint as a safeguard against executive abuse—has remained a focal point in the continuing debate over national security surveillance.

III. CONGRESSIONAL AND JUDICIAL REGULATION OF NATIONAL SECURITY SURVEILLANCE UNDER THE FOURTH AMENDMENT

A. Title III Warrants for Electronic Surveillance

After *Katz*, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[37] Title III provided a procedure for government agents to obtain judicial approval to intercept wire, oral, and electronic communications.[38]

The requirements of Title III closely track the traditional Fourth Amendment warrant requirements. In order to issue a Title III warrant, a judge must receive a written application upon oath or affirmation of a law

---

[32] *Id*. at 358 n.23.
[33] *Id.* at 363−64 (White, J., concurring).
[34] *Id*. at 359 (Douglas, J., concurring).
[35] *Id*.
[36] *Id*. at 359–60.
[37] Pub. L. No. 90-351, §§ 801–804, 82 Stat. 197, 211–25 (1968).
[38] 18 U.S.C. §§ 2516–2518 (2000 & West Supp. 2005).

enforcement officer.[39] The judge must then find probable cause to believe that an individual is committing, has committed, or is about to commit a particular crime.[40] The judge must also find probable cause to believe that particular communications about the crime will be obtained, and that the facility targeted for surveillance is being used or is about to be used in connection with the crime or by the person suspected of the crime.[41] Finally, the judge must determine that "normal investigative procedures" other than electronic surveillance have failed or are unreasonable for some reason.[42]

Title III contains several provisions designed to minimize the invasion of privacy when a warrant is issued. For example, Title III limits surveillance orders to thirty days.[43] Surveillance may only be extended by going through the initial application procedure.[44] Within ninety days, the target of the surveillance, and in some cases other individuals whose communications were intercepted, must be notified of the surveillance.[45] Title III also requires the government to adhere to procedures designed to minimize the interception of communications that do not relate to the crime or that involve participants not connected to the criminal activity.[46]

Title III does not regulate national security surveillance. In fact, Congress specifically excluded such surveillance from the scope of the legislation:

> Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.[47]

B. The Keith *Case: Applying the Fourth Amendment to Domestic Security Surveillance*

The Supreme Court first addressed national security surveillance in a 1972 decision, *United States v. United States District Court*.[48] This case is commonly referred to as the "*Keith*" case after the district court judge mandamused by the government. The *Keith* case involved the criminal trial of individuals charged with bombing a CIA office in Ann Arbor, Michigan.[49] The government

---

[39] 18 U.S.C. § 2518(1).

[40] *Id*. § 2518(3)(a). In order to obtain a Title III warrant, the suspected crime must be one of a number of enumerated offenses under 18 U.S.C. § 2516(1).

[41] *Id*. § 2518(3)(b), (d).

[42] *Id*. § 2518(3)(c).

[43] *Id*. § 2518(5).

[44] *Id*.

[45] *Id*. § 2518(8)(d).

[46] *Id*. § 2518(5).

[47] 18 U.S.C. § 2511(3) (1976), *repealed by* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 201(c), 92 Stat. 1783, 1797.

[48] 407 U.S. 297 (1972) [hereinafter *Keith*].

[49] *Id*. at 299.

admitted that it had conducted warrantless electronic surveillance of the defendant,[50] but argued that the surveillance was lawful because its purpose was "'to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government.'"[51]

The District Court for the Eastern District of Michigan rejected the government's argument and held that the surveillance violated the Fourth Amendment because it was conducted without prior judicial approval.[52] The government filed a petition for writ of mandamus against Judge Keith. The Court of Appeals for the Sixth Circuit affirmed the lower court. The Supreme Court granted review on the narrow question left open by *Katz*: "'Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security . . . .'"[53]

The Supreme Court held that the government must seek judicial approval before conducting electronic surveillance for domestic security purposes.[54] In reaching this conclusion, the Court balanced the President's duty to protect the nation from overthrow against the privacy interests of individuals.[55] The Court set out a framework to decide the issue:

> If the legitimate need of Government to safeguard domestic security requires the use of electronic surveillance, the question is whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant before such surveillance is undertaken. We must also ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it.[56]

Notably, the Court's Fourth Amendment analysis focused not merely on the security needs underlying the surveillance, but also on whether it would have been reasonable to require a warrant prior to conducting the surveillance.[57]

The Court concluded that the needs of citizens for privacy and free expression would be better served by requiring a warrant prior to surveillance.[58] The Court stated that national security surveillance represents an area of "convergence of First and Fourth Amendment values,"[59] and thus presents a great risk of abuse, particularly by targeting political dissenters: "History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute

---

[50] *Id*. at 300.
[51] *Id*. (quoting Affidavit of Attorney General).
[52] *Id*. at 301.
[53] *Id*. at 309 (quoting Katz v. United States, 389 U.S. 347, 358 n.23 (1967)).
[54] *Id*. at 321.
[55] *Id*. at 315.
[56] *Id*.
[57] *Id*.
[58] *Id*. at 321.
[59] *Id*. at 313.

its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs."[60]

The Court considered and rejected each of the government's arguments that domestic security surveillance should constitute an exception to the warrant requirement.[61] First, the government argued that domestic security surveillance is ill-suited to the traditional warrant requirement because it is targeted at collecting and maintaining intelligence rather than acquiring evidence of specific criminal activity.[62] The Court stated that this interest was not sufficient to justify a departure from Fourth Amendment standards given the significant temptation for abuse.[63] Second, the government argued that courts "'as a practical matter would have neither the knowledge nor the techniques necessary to determine whether there was probable cause to believe that surveillance was necessary to protect national security.'"[64] The Court responded by stating:

> We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society . . . . If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.[65]

The Court limited its holding in two ways. First, the Court pointed out that its opinion did not extend to surveillance that involves the activities of "foreign powers or their agents."[66] This differentiation between domestic threats to national security and threats with a foreign connection is significant in the enactment of the Foreign Intelligence Surveillance Act.[67]

Second, the Court stated that, while the "warrant" requirement applies to national security surveillance, the form of prior judicial approval may vary from Title III standards due to the inherent differences between ordinary criminal surveillance and national security surveillance.[68] For example, the complex task of gathering security information sometimes requires longer-term surveillance, and the exact targets of the surveillance may be difficult to

---

[60] *Id*. at 314. The Court quoted from the floor debate on Title III: "As I read it—and this is my fear—we are saying that the President, on his motion, could declare—name your favorite poison—draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure or existence of the Government." *Id*. (quoting 114 CONG. REC. 14750 (1967) (statement of Sen. Hart)).

[61] *Id*. at 318–20.

[62] *Id*. at 318–19.

[63] *Id*. at 320.

[64] *Id*. at 319 (quoting Reply Brief for United States at 4).

[65] *Id*. at 320.

[66] *Id*. at 321–22.

[67] *See infra* Part IV (discussing enactment of the Foreign Intelligence Surveillance Act).

[68] *Keith*, 407 U.S. at 322.

identify in national security cases.[69] In addition, national security surveillance generally aims to prevent future unlawful activity and to enhance government preparedness, rather than to obtain evidence of past crimes for prosecution.[70] The Court encouraged Congress to adopt new warrant procedures specifically for national security surveillance that would take these differences into account:

> It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of [Title III] but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court . . . and that the time and reporting requirements need not be so strict as those in [Title III].[71]

C. The Application of Keith *to Foreign Intelligence Surveillance*

In many ways, *Keith* did more to confuse the application of the Fourth Amendment to national security surveillance than it did to clarify it. The Court held that national security surveillance is not exempt from prior judicial approval when targeted at a domestic organization. However, it created a distinction between domestic and foreign intelligence surveillance that did not previously exist, and it failed to define the distinction either in terms of the type of threat required or the government interest involved. The Court imposed a warrant requirement but sanctioned warrant procedures that are "different" than those implemented by Title III, leaving for later decision what type of differences may be constitutionally reasonable.

Most importantly, *Keith* expressly refused to state whether foreign intelligence surveillance also requires prior judicial approval, leaving the various circuit courts to grapple with this important question. Most courts agreed that foreign intelligence surveillance, as compared to domestic security surveillance, constituted an exception to the warrant requirement.[72]

Only one court, the Court of Appeals for the District of Columbia, questioned whether foreign intelligence surveillance justifies an exception to the warrant requirement.[73] In *Zweibon v. Mitchell*, the Jewish Defense League (JDL) challenged numerous warrantless surveillances in a *Bivens* suit against

---

[69] *Id*.

[70] *Id*.

[71] *Id*. at 323.

[72] *See, e.g.*, United States v. Brown, 484 F.2d 418 (5th Cir. 1973) (holding that the Fourth Amendment permits warrantless surveillance as long as the Attorney General certifies that the purpose of the surveillance is to gather foreign intelligence information); United States v. Butenko, 494 F.2d 593 (3d Cir. 1974) (holding that the Fourth Amendment permits warrantless surveillance as long as its sole purpose is to gather foreign intelligence information and any accumulation of evidence of criminal activity is incidental); United States v. Buck, 548 F.2d 871 (9th Cir. 1977) (holding that the Fourth Amendment permits warrantless surveillance as long as in camera review reveals that the purpose of the surveillance is to gather foreign intelligence information).

[73] Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975).

the government.[74] The government responded that surveillance of the JDL did not require a warrant because it was foreign intelligence surveillance.[75] The government argued that the activities of the JDL involved foreign affairs because they were "detrimental to the continued peaceful relations between the United States and the Soviet Union . . . ."[76]

Sitting en banc, the court examined the possible justifications to exempt foreign intelligence surveillance from the warrant requirement.[77] The plurality opinion stated: "[W]e believe that an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional . . . ."[78] However, the court's holding, endorsed by four judges of the eight-judge panel, stated only that the government must obtain a warrant prior to conducting surveillance of a completely domestic organization that is not acting in collaboration with a foreign power.[79]

D. United States v. Truong Dinh Hung *and the Genesis of the Primary Purpose Test*

In contrast to the D.C. Circuit plurality's analysis in *Zweibon*, the Court of Appeals for the Fourth Circuit, in *United States v. Truong Dinh Hung*,[80] held that foreign intelligence surveillance does constitute an exception to the warrant requirement.[81] Although *Truong* was decided in 1980, after the enactment of the Foreign Intelligence Surveillance Act of 1978 (FISA),[82] the government surveillance took place in 1977, so the court did not address the FISA statute.[83] In *Truong*, the defendant was convicted of transmitting classified government information to the Socialist Republic of Vietnam.[84] The defendant challenged the prosecution's use of information obtained through warrantless electronic surveillances.[85] The district court allowed the prosecution to use information obtained by the government when its investigation was "primarily a foreign intelligence investigation," but it excluded evidence obtained after the FBI investigation had become "primarily a criminal investigation."[86]

The Fourth Circuit affirmed the district court and held that foreign intelligence surveillance qualifies as an exception to the Fourth Amendment

---

[74] *Id*. at 605.
[75] *Id*. at 607.
[76] *Id*. at 607–08.
[77] *Id*. at 637–51.
[78] *Id*. at 613−14.
[79] *Id.* at 614.
[80] 629 F.2d 908 (4th Cir. 1980).
[81] *Id*. at 914.
[82] *See infra* Part IV (discussing enactment of the Foreign Intelligence Surveillance Act of 1978).
[83] *Truong*, 629 F.2d at 912.
[84] *Id*. at 911.
[85] *Id*. at 912.
[86] *Id*. at 912−13.

only when (1) the target of the surveillance is a foreign power, its agent, or collaborators; and (2) the surveillance is conducted primarily for foreign intelligence reasons and not primarily for a criminal investigation.[87]

The *Truong* court followed the analytical framework set out in *Keith*.[88] However, the court found three differences between foreign intelligence surveillance and domestic security surveillance that suggested a warrant requirement would unduly frustrate the President in protecting national security from foreign threats. First, foreign intelligence surveillance requires "the utmost stealth, speed, and secrecy."[89] Second, the judiciary is largely inexperienced in analyzing foreign intelligence information.[90] And third, the Executive Branch is constitutionally imbued with preeminent authority to conduct foreign affairs.[91] Because of these distinctions, the court held that foreign intelligence surveillance constituted an exception to the general warrant requirement.[92]

However, the court recognized the delicacy of the balance that exists between the government's interests and the risks to individual privacy.[93] Therefore, the court held that foreign intelligence surveillance only constitutes a warrant exception when the government's need for flexibility is at the fore: namely, when the target of the search is a foreign power or agent and when the surveillance is conducted *primarily* for foreign intelligence reasons.[94] When the investigation is primarily criminal "individual privacy interests come to the fore," and "courts are entirely competent to make the usual probable cause determination."[95]

In imposing the "primary purpose" test, the *Truong* court expressly rejected the tests proposed by both the government and the defendant.[96] The government argued that foreign intelligence surveillance should be exempted from the warrant requirement whenever the surveillance implicates foreign intelligence to any degree.[97] The court held that this formulation did not adequately balance the individual privacy interests and the court's ability to determine probable cause for ordinary criminal surveillance.[98] The defendant argued that surveillance should only be exempted when it is conducted "solely" for foreign policy reasons.[99] The court rejected this formulation because it

[87] *Id*. at 915.
[88] *Id*. at 913.
[89] *Id*.
[90] *Id*. at 913−14.
[91] *Id*. at 914 (citing First Nat'l City Bank v. Banco Nacional de Cuba, 406 U.S. 759 (1972)); *see also* Oetjen v. Cent. Leather Co., 246 U.S. 297 (1918).
[92] *Id.* at 915.
[93] *Id*.
[94] *Id*.
[95] *Id*.
[96] *Id*. at 915–16.
[97] *Id*.
[98] *Id*.
[99] *Id*.

would not fulfill the government's need for flexibility and control.[100] The court quoted the testimony of Attorney General Bell, who stated: "Let me say that every one of these counterintelligence investigations involved, nearly all of them that I have seen, involves crime in an incidental way."[101]

Truong is widely credited with establishing the primary purpose test, a test that continued to maintain importance even after the enactment of FISA.

IV. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) OF 1978

A. Enactment of FISA

Amidst the judicial confusion surrounding national security surveillance and the appropriate scope of the Fourth Amendment, the Executive Branch continued to conduct warrantless surveillance for foreign intelligence.[102]

In 1975, Congress commissioned a committee headed by Senator Frank Church to investigate executive abuse of warrantless surveillance.[103] The investigation of the "Church Committee" revealed excessive use and abuse of unregulated intelligence surveillance targeted at U.S. citizens.[104] Many targets were not even suspected of crimes, nor were they perceived as violent.[105] For example, targets of the surveillance included political dissenters, anti-Vietnam War organizations, and civil rights leaders such as Martin Luther King, Jr. [106] The scope of the problem was immense.[107] In 1972 alone, the FBI opened sixty-five thousand domestic intelligence files.[108] The Church Committee found that this type of investigation was conducted with complete disregard for legal and constitutional restraints.[109]

The Church Committee recommended that Congress pass legislation to regulate these searches and to prevent further abuse.[110] In 1978, Congress followed the Church Committee's recommendations and passed FISA.[111] Like Title III, which provided a procedure for electronic wiretapping to obtain evidence of ordinary crimes, FISA provided a procedure for the government to conduct electronic surveillance for foreign intelligence and counterintelligence

---

[100] *Id*.

[101] *Id*. at 916 n.5.

[102] *See generally* S. REP. NO. 95-604, at 1–15 (1978) (describing history of national security surveillance and explaining the need for regulation).

[103] CHURCH COMMITTEE REPORT, BOOK II, *supra* note 13.

[104] *Id*, at 5–20.

[105] *Id*. at 68.

[106] *Id*. at 71–75.

[107] *See generally id*. at 5–20 (summarizing the scope of the problem of executive intelligence abuse).

[108] *Id*. at 6.

[109] *Id*. at 13.

[110] *Id*. at 296.

[111] Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (1978).

reasons.[112] However, unlike Title III, the method of judicial approval mandated by FISA radically departed from the traditional warrant requirements.[113]

1. The Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review

FISA established an entirely new court, known as the Foreign Intelligence Surveillance Court (FISC).[114] The FISC consists of eleven federal judges appointed by the Chief Justice, each of whom serves non-renewable terms of seven years.[115] The FISC's sole jurisdiction consists of hearing applications and granting orders approving electronic surveillance.[116] FISA also established an appellate court, known as the Foreign Intelligence Surveillance Court of Review (FISCR).[117] The FISCR consists of three federal judges, also appointed by the Chief Justice, who serve non-renewable terms of seven years.[118] The FISCR's sole jurisdiction consists of reviewing the denial of any FISA application.[119] The FISCR has only heard one case since the enactment of FISA.[120]

2. FISA Application Process

A FISA application must contain a description of the target of the surveillance, and a statement of facts justifying belief that the target is a foreign power or agent of a foreign power.[121] The application must also contain a

[112] 50 U.S.C. §§ 1801–1806 (2000). "Counterintelligence" is defined as "information deemed necessary to the nation's ability to discover and protect against the activities of clandestine intelligence services of foreign powers in the United States." S. REP. NO. 95-604, at 32 (1978).

[113] *Compare* 50 U.S.C. §§ 1801–1806 (laying out procedures for foreign intelligence surveillance) *with* 18 U.S.C. §§ 2516–2518 (2000) (laying out procedures for surveillance involving serious crimes).

[114] 50 U.S.C. § 1803(a).

[115] *Id*. § 1803(a), (d). As originally enacted, the FISC consisted of seven judges, Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, § 103, 92 Stat. 1783, 1788, but that number was later increased to eleven. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, § 208, 115 Stat. 272, 283 (2001) [hereinafter Patriot Act].

[116] 50 U.S.C. § 1803(a).

[117] *Id*. § 1803(b).

[118] *Id*. § 1803(b), (d).

[119] 50 U.S.C. § 1803(b).

[120] *See infra* Part VI (discussing *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002)).

[121] 50 U.S.C. § 1804(a)(4) (2000). A "foreign power" includes:

> (1) a foreign government or any component thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> (4) a group engaged in international terrorism or activities in preparation therefor;
>
> (5) a foreign-based political organization, not substantially composed of United States persons; or
>
> (6) an entity that is directed and controlled by a foreign government or governments.

statement justifying the belief that the target facility is being used or is about to be used by a foreign power or an agent of a foreign power.[122] The original version of FISA required certification by a high-level executive official that the information sought in the surveillance is foreign intelligence information, that the purpose of the surveillance is to obtain foreign intelligence information, and that the information cannot be obtained by normal investigative techniques.[123]

Finally, the FISA application must contain a statement of the proposed minimization procedures to be followed by the government.[124] Minimization procedures are procedures "which shall be adopted by the Attorney General" that are designed to minimize the acquisition, retention, and dissemination of nonpublic information obtained in FISA surveillance that is not foreign intelligence information, particularly with respect to concealing the identity of any United States person (citizen or lawful permanent resident[125]) involved in the surveillance.[126] However, information obtained through FISA surveillance

50 U.S.C. § 1801(a) (2000). An "agent of a foreign power" includes, among others, anyone who:

> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power.

50 U.S.C. § 1801(b)(2). "International terrorism" includes activities that "involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State." 50 U.S.C. § 1801(c)(1).

[122] 50 U.S.C. § 1804(a)(3)–(4) (2000).

[123] Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, §§ 103, 104(a)(7)(A)-(C), 92 Stat. 1783, 1788-89 (1978). This section was amended by section 218 of the Patriot Act requiring certification that obtaining foreign intelligence information is "a significant purpose" of the surveillance instead of "the purpose" of the surveillance. "Foreign intelligence information" is:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to –
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e).

[124] 50 U.S.C. § 1804(a)(5).

[125] *Id*. § 1801(i).

[126] *Id*. § 1801(h)(1)–(2).

that is evidence of a crime can be "retained or disseminated for law enforcement purposes."[127]

3. Judicial Review

Upon receiving an application certified by the Attorney General, as required, the FISA court must approve an order for surveillance "as requested or as modified" if the court determines that there is probable cause to believe that the target of the surveillance is a foreign power or agent of a foreign power, and that the facility surveilled is being used or is about to be used by a foreign power or an agent of a foreign power.[128] If the target of the surveillance is a United States person, the court's determination that the target is a foreign power or agent of a foreign power cannot be made "solely upon the basis of activities protected by the [F]irst [A]mendment."[129]

Normally, the FISA judge may not review the agent's certification that the purpose of the surveillance is to obtain foreign intelligence information. The certification is subject to review only when the surveillance targets a U.S. citizen, in which case the certification would be reviewed for clear error.[130]

4. Expiration and Notice

FISA orders last for ninety days when the target is an agent of a foreign power, and can last for up to one year if the target is a foreign power.[131] Extensions may be granted for up to one year.[132] Importantly, FISA does not require the government to notify targets of FISA surveillance that communications were intercepted unless the person is charged with a crime and the government intends to use surveillance evidence in the prosecution.[133]

B. Judicial Interpretation of FISA under the Fourth Amendment

FISA allows the Executive Branch to conduct foreign intelligence surveillance with the sanction of prior judicial approval. However, FISA review of surveillance applications clearly differs from the review mandated under the traditional Title III warrant procedure. This incongruity raises new questions: Do FISA procedures for national security surveillance comply with the Fourth Amendment? Do the procedures strike a constitutionally acceptable balance between the needs of the government and the Fourth Amendment's protection of individual privacy?

Federal district and appellate courts have come up with several answers. Some courts have held that compliance with FISA procedures satisfies the Fourth Amendment.[134] Other courts have held that compliance with FISA

---

[127] *Id.* § 1801(h)(3).
[128] *Id.* § 1805(a)(3)(A)–(B).
[129] *Id.* § 1805(a)(3)(A).
[130] *Id.* § 1805(a)(5).
[131] *Id.* § 1805(e)(1).
[132] *Id.* § 1805(e)(2).
[133] 50 U.S.C. § 1806(c) (2000).
[134] *See, e.g.*, United States v. Falvey, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982).

procedures satisfies the Fourth Amendment only when the primary purpose of the surveillance is foreign intelligence.[135] In *United States v. Duggan*,[136] the Second Circuit affirmed the latter rationale, upholding FISA surveillance that met the primary purpose standard. In *United States v. Sarkissian*,[137] the Ninth Circuit followed the former approach and held that compliance with FISA procedures satisfied the Fourth Amendment. The Ninth Circuit cautioned that courts should not draw too fine a distinction between investigations for foreign intelligence, as opposed to criminal purposes, since foreign counterintelligence surveillance inherently involves investigation of crimes.[138]

C. Coordination Between Law Enforcement and Intelligence Officers and "the Wall"

The Department of Justice (DOJ) followed the primary purpose test.[139] The DOJ interpreted the primary purpose test as prohibiting criminal prosecutors from directing or controlling FISA surveillance.[140] In the early 1990s, the DOJ's Office of Intelligence and Policy Review (OIPR), the office responsible for submitting FISA applications to the FISC, became concerned that consultations between FBI agents and prosecutors may lead to the appearance that the agents were using FISA surveillance for criminal purposes.[141] If courts thought that agents were using FISA surveillance primarily for criminal prosecution, it would jeopardize the DOJ's ability to use evidence obtained in FISA surveillance in a later prosecution.

In response to these concerns, Attorney General Janet Reno implemented formal procedures for the flow of information from foreign intelligence investigations to criminal prosecutors.[142] The 1995 Procedures allowed intelligence officers to provide information regarding ongoing FISA surveillance to law enforcement officers only when the investigation indicated "significant federal criminal activity."[143] The procedures forbade law enforcement officers from taking any action that would result in "either the fact or the appearance" of the law enforcement officers "directing or controlling" the foreign intelligence investigation for law enforcement purposes.[144]

---

[135] *See, e.g.*, United States v. Megahey, 553 F. Supp. 1180, 1189 (E.D.N.Y. 1982), *aff'd*, United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

[136] 743 F.2d 59, 78 (2d Cir. 1984).

[137] 841 F.2d 959, 965 (9th Cir. 1988).

[138] *Id*. The court relied on the statement of Attorney General Bell in *Truong* where he was quoted as saying that all foreign counterintelligence investigations involve crime in at least an incidental way. *See supra* note 101.

[139] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 78 (2004) [hereinafter 9/11 COMMISSION REPORT].

[140] *Id*.

[141] *Id*.

[142] *Id*. at 79.

[143] Memorandum from Janet Reno, U.S. Att'y Gen., to Assistant Att'y Gen., Criminal Div. (July 19, 1995) [hereinafter 1995 Procedures], *available at* http://www.fas.org/irp/agency/doj/fisa/1995procs.html.

[144] *Id*. at 2, para. 6.

However, law enforcement officers were not prohibited from consulting with intelligence officers concerning the investigations.[145]

As a result of a confluence of factors, the DOJ went beyond the requirements of the 1995 Procedures and cut off the flow of any intelligence information to criminal prosecutors. The DOJ also prevented such information from flowing to FBI agents who were involved in criminal investigations.[146] The DOJ procedures, in practice, ensured that foreign intelligence was not just the primary purpose of any FISA surveillance, but that it was the exclusive purpose. These barriers to information sharing became known as "the Wall."[147] After the terrorist attacks of September 11, Congress found that lack of coordination within the DOJ may have contributed to the government's inability to capitalize on mistakes made by the terrorists prior to the attacks.[148]

V. THE PATRIOT ACT AMENDMENTS TO FISA AND THE DISSOLUTION OF THE PRIMARY PURPOSE TEST

A. September 11 and the Patriot Act

On September 11, 2001, terrorists conducted a massive attack on American soil. Nineteen hijackers took control of four commercial passenger jets containing cross-country fuel loads, and crashed the jets into the World Trade Center towers in New York City, the Pentagon in Washington, D.C., and an empty field in Shanksville, Pennsylvania.[149] The death toll, while inexact, was estimated to be at least 3,000.[150]

Congress hastily responded to the attacks by immediately drafting and enacting legislation to "provide … enhanced investigative tools and improve … information sharing for the law enforcement and intelligence communities to combat terrorism[.]"[151] The legislation, passed forty-five days after September 11, was entitled the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" Act, or the USA PATRIOT Act.[152] The Patriot Act granted law enforcement and

---

[145] *Id*. at 2, para. 5.

[146] 9/11 COMMISSION REPORT, *supra* note 139, at 79.

[147] *Id*.

[148] *Id*. at 263–77. *See infra* Part V (discussing the role of the primary purpose test in intelligence failures).

[149] 9/11 COMMISSION REPORT, *supra* note 139, at 4−14.

[150] Lists of Victims, http://www.cnn.com/SPECIALS/2001/trade.center/victims/main.html (last visited May 18, 2006); Sara Kugler, *New WTC Death Toll is 2,752*, CBSNEWS.COM, Oct. 30, 2003, http://www.cbsnews.com/stories/2003/10/29/attack/main580620.shtml.

[151] H.R. REP. NO. 107-236, pt. 1, at 52–76 (2001).

[152] Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

intelligence agencies expanded powers, including the authorization to use roving wiretaps, internet tracking, and "sneak-and-peek" searches.[153]

The Patriot Act made numerous amendments to FISA, two of which were specifically targeted at solving the coordination problems in the DOJ that had developed into the Wall. First, the Patriot Act amended the purpose requirement, now requiring foreign intelligence information to be "a significant purpose" of the surveillance, rather than "the purpose" of the surveillance.[154] Second, the Patriot Act authorized foreign intelligence officers to "consult with Federal law enforcement officers to coordinate efforts to investigate or protect against" foreign intelligence crimes.[155] Coordination of this type "shall not preclude" agents from certifying that foreign intelligence information is still "a significant purpose" of the surveillance.[156]

Congress intended these amendments to clear up any confusion regarding coordination between law enforcement and intelligence agencies, but the amendments fell prey to varying interpretations. One interpretation of these amendments is that they merely clarified that foreign intelligence need not be the exclusive purpose of FISA surveillance. Under this interpretation, the amendments would alleviate the OIPR's concerns that consultations between prosecutors and intelligence agents would automatically result in the denial of a FISA order. The amendments would still preserve the rule that prosecutors may not direct or control FISA surveillance, and more importantly, that FISA surveillance may not be conducted when the primary purpose of the surveillance is criminal prosecution. In other words, the DOJ would merely revert back to using Attorney General Reno's original 1995 Procedures.

Another interpretation of these amendments is that they eliminated the primary purpose requirement altogether by allowing complete coordination between law enforcement and criminal prosecutors. Under this interpretation, the government may conduct FISA surveillance even when criminal prosecution is its primary objective, as long as intelligence gathering is still a significant purpose.

Predictably, the Department of Justice advocated the latter view since it would significantly increase the government's ability to use FISA surveillance in situations when it has simultaneous, ongoing criminal and intelligence investigations.[157] The DOJ, through Attorney General John Ashcroft, took this interpretation to the FISC in May 2002 and asked the court to approve new "Intelligence Sharing Procedures."[158] Unlike the 1995 Procedures, the 2002

---

[153] *Id*. §§ 206 (roving surveillance authority), 217 (interception of computer trespasser communications), 213 ("sneak-and-peak" warrants).

[154] *Id*. § 218.

[155] *Id*. § 504.

[156] *Id*.

[157] Memorandum from John Ashcroft, U.S. Att'y Gen., to Director, FBI (Mar. 6, 2002) [hereinafter 2002 Procedures], *available at* http://www.fas.org/irp/agency/doj/fisa/ag030602.html.

[158] *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 262 F. Supp. 611, 613 (FISA Ct. 2002) [hereinafter *In re All Matters*].

Procedures allowed complete exchange between the FBI and the Criminal Division regarding "the initiation, operation, continuation, or expansion of FISA searches or surveillance."[159] The FISC rejected the new procedures offered by the DOJ.

B. In re Sealed Case*, The Foreign Intelligence Surveillance Court of Review's First Opinion*

Undeterred by the FISC's chilly reception to its proposed procedures, the government appealed the decision to the Foreign Intelligence Surveillance Court of Review (FISCR), providing that court with its first case.[160] On appeal, the statutory question was whether the primary purpose test should still apply after the Patriot Act amendments. The constitutional question was whether FISA, interpreted without the primary purpose test, would pass muster under the Fourth Amendment.[161]

The FISCR heard the government's oral presentation on September 9, 2002, just shy of two days before the anniversary of the September 11 attacks.[162] The three federal judges agreed with the government and reversed the lower court, holding not only that the Patriot Act amendments eliminated the primary purpose requirement as a matter of statutory interpretation,[163] but also that FISA procedures satisfy the Fourth Amendment, even when the primary purpose of the surveillance is criminal prosecution and not foreign intelligence.[164]

The FISCR's Fourth Amendment analysis is of primary importance for the present discussion, but one key point of its statutory analysis also requires explanation. The FISCR interpreted the Patriot Act amendments to allow FISA surveillance when foreign intelligence *is not* the primary purpose of the surveillance, but it also interpreted the statute to allow FISA surveillance when criminal prosecution *is* the primary purpose. The FISCR reached this conclusion by analyzing the statute's definition of "foreign intelligence information."[165] As defined by FISA, "foreign intelligence information" includes information necessary to protect the country against attack, sabotage, international terrorism, or espionage by a foreign power or an agent of a foreign power.[166] The court termed these crimes "foreign intelligence crimes."[167] The

---

[159] 2002 Procedures, *supra* note 157, § II(B).

[160] *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002).

[161] Because FISA proceedings are conducted *ex parte*, the FISCR accepted briefs from *amici curiae*, the American Civil Liberties Union (ACLU) and the National Association of Criminal Defense Lawyers, to argue against the government.

[162] The Solicitor General, Ted Olson, presented the government's case. Solicitor General Olson's wife, Barbara Olson, was a passenger on American Airlines Flight 77, the plane that terrorists crashed into the Pentagon, making his presentation of the case particularly poignant. 9/11 COMMISSION REPORT, *supra* note 139, at 9.

[163] *In re Sealed Case*, 310 F.3d at 734.

[164] *Id*. at 746.

[165] *Id*. at 723–34.

[166] 50 U.S.C. § 1801(e)(1) (2000).

court reasoned that FISA would not have authorized the government to conduct surveillance to protect the country against foreign intelligence crimes without allowing the government to accomplish that task by criminal prosecution.[168]

From this conclusion, the FISCR rejected the government's contention that this extends to the prosecution of "ordinary crimes" with only an incidental link to foreign intelligence information.[169] The court held that FISA permits a surveillance order when the purpose is to prosecute "ordinary crimes" only when the crimes are "inextricably intertwined with foreign intelligence crimes," such as the hypothetical case where terrorists engage in bank robbery to fund a terrorist attack.[170]

On the constitutional question, the FISCR relied on the Supreme Court's dicta in *Keith* to hold that even though FISA requirements diverge from Title III requirements in constitutionally relevant areas, the FISA procedures satisfy the Fourth Amendment. The FISCR held that the procedures meet the Fourth Amendment's requirements because they are reasonable in light of the special needs of government in conducting foreign intelligence surveillance.[171]

The FISCR's Fourth Amendment analysis is particularly remarkable for its categorical rejection of the primary purpose test, notwithstanding the fact that the primary purpose test had dominated FISA analysis for the past quarter century.[172] The court held that the primary purpose test creates an "inherently unstable, unrealistic, and confusing" line between law enforcement and foreign intelligence purposes,[173] pointing out that the creation of the Wall and the subsequent confusion and conflict within the DOJ may have played a part in several well-publicized intelligence failures,[174] including 9/11: "[T]he FISA court requirements based on *Truong* may well have contributed, whether correctly understood or not, to the FBI missing opportunities to anticipate the September 11, 2001 attacks."[175]

The court also disagreed with the *Truong* court's reason for imposing the primary purpose test, its belief that the government's foreign policy concerns recede when the primary purpose of surveillance is criminal prosecution.[176] The FISCR noted that effective prosecution is an important part of counterintelligence because it is one method to prevent or terminate the commission of foreign intelligence crimes.[177] In this light, government foreign

---

[167] *In re Sealed Case*, 310 F.3d at 723.

[168] *Id*. at 727.

[169] *Id*. at 735–36.

[170] *Id*. at 736.

[171] *Id*. at 746.

[172] *Id*. at 742–45.

[173] *Id*. at 743.

[174] *See, e.g.*, ATT'Y GEN.'S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NAT'L LAB. INVESTIGATION, U.S. DEP'T OF JUSTICE, THE BELLOWS REPORT (2000), *available at* http://www.usdoj.gov/ag/readingroom/bellows.htm (detailing impediments to coordination in the Los Alamos investigation of Wen Ho Lee).

[175] *In re Sealed Case*, 310 F.3d at 744.

[176] *Id*. at 743.

[177] *Id*.

policy concerns do not necessarily recede simply because prosecution is contemplated.[178]

The court thus jettisoned the traditional rubric under which FISA surveillance had previously been analyzed, discarding the existing dichotomy between foreign intelligence and law enforcement purposes as irrational. Having effectively cleared the slate, the court went on to consider whether FISA procedures are a "reasonable response based on a balance of the legitimate need of the government for foreign intelligence information . . . with the protected rights of citizens" as required by the *Keith* decision.[179]

The court first compared FISA procedures to Title III procedures, reasoning that the closer the two matched, the more easily it could find that FISA procedures are reasonable under the Fourth Amendment.[180] But the court concluded that the procedures were too different to provide an accurate comparison.[181] Both provided the critical elements of probable cause, particularity, and issuance by a neutral and detached magistrate, but the statutes operated in such different settings that comparison of the two would be unavailing.[182]

At this juncture, if the FISCR had determined that FISA orders are equivalent to Title III warrants, the Fourth Amendment question would be essentially satisfied. Instead, the FISCR concluded that the orders may not be "warrants" in the Fourth Amendment sense, requiring the court to determine whether FISA surveillance qualifies for a warrant exception. The court addressed this matter only by stating: "to the extent the two statutes diverge in constitutionally relevant areas . . . a FISA order may not be a 'warrant' contemplated by the Fourth Amendment."[183]

The court finally turned to the Supreme Court's "special needs" exception to the warrant requirement. [184] The Supreme Court has held that the Fourth Amendment requirement of individualized suspicion may be suspended in certain cases in order to serve the government's "'special needs, beyond the normal need for law enforcement.'"[185] The Supreme Court has held that programs serving a special need may be upheld if the procedures reasonably balance the severity of the privacy intrusion with the public interest served by the program.[186] To determine whether a government program qualifies for a warrant exception under the special needs doctrine, courts must first determine

---

[178] *Id*.

[179] *Id*. at 742.

[180] *Id*. at 737–42.

[181] *Id*. at 741.

[182] *Id*.

[183] *Id*.

[184] *Id*. at 745–46.

[185] *Id*. at 745 (quoting Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)); *see also* Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990); City of Indianapolis v. Edmond, 531 U.S. 32 (2000); Illinois v. Lidster, 540 U.S. 419 (2003).

[186] *Lidster*, 540 U.S. at 426–27.

whether the interest served is a special need.[187] Then, courts must conduct a balancing test to determine whether the warrantless searches are reasonable.[188]

Relying on its own definition of the government's interest—the interest in protecting the country against foreign intelligence crimes committed by foreign powers and their agents—the FISCR held that this interest qualifies as a special need.[189] The court held that, even though FISA surveillance may involve gathering evidence for criminal prosecution, its programmatic purpose is to protect citizens against a specific hazard, and this purpose goes beyond the normal need for law enforcement.[190] The court also held that FISA procedures provide significant protection to individuals.[191] The FISCR concluded: "We, therefore, believe firmly, applying the balancing test drawn from *Keith*, that FISA as amended is constitutional because the surveillances it authorizes are reasonable."[192]

The Supreme Court denied the ACLU leave to intervene in order to file a petition for writ of certiorari of the *In re Sealed Case* decision, making the FISCR's opinion final.[193]

VI. *IN RE SEALED CASE* AND THE FOURTH AMENDMENT'S REASONABLENESS REQUIREMENT

The FISCR's decision in *In re Sealed Case* is a well-reasoned and plausible application of the Fourth Amendment to national security surveillance. It rejected the primary purpose test based on valid concerns regarding cooperation between various government agencies charged with protecting national security. The court then applied the Supreme Court's *Keith* decision to FISA procedures and held that the procedures reasonably balance the legitimate needs of the government to obtain intelligence information with the privacy rights of citizens. Furthermore, the court followed the Supreme Court in its recent inclination to expand the special needs doctrine to find a warrant exception for national security surveillance.

Nevertheless, the *In re Sealed Case* decision leaves a bad taste in the mouths of civil libertarians and Fourth Amendment scholars. This section of the Comment analyzes possible concerns raised by *In re Sealed Case*. First, this section will discuss the possibility that the *In re Sealed Case* decision authorizes the government to make an end run around Fourth Amendment requirements in areas traditionally recognized as law enforcement and provides a breeding ground for executive abuse. Second, this section discusses how the FISCR's application of the special needs doctrine presents the risk of expanding that doctrine to engulf the warrant requirement. Finally, in light of

187 *Id*. at 426.
188 *Id*. at 426.
189 *In re Sealed Case*, 310 F.3d at 746.
190 *Id*.
191 *Id*.
192 *Id*.
193 ACLU v. United States, 538 U.S. 920 (2003).

these concerns, this section concludes that the *In re Sealed Case* decision violates the Fourth Amendment because it authorizes government surveillance that is unreasonable.

A. In re Sealed Case Expands the Government's Ability to Use FISA Surveillance as an End Run Around Traditional Fourth Amendment Requirements in Criminal Prosecutions

The *In re Sealed Case* decision significantly expands federal prosecutors' ability to use FISA surveillance in criminal prosecutions. Prior to *In re Sealed Case*, prosecutors were restricted from directing or controlling FISA surveillance, and prosecutors were only involved in receiving information relating to FISA when it involved "significant criminal activity." As a result of *In re Sealed Case*, prosecutors may now use FISA surveillance as a tool for prosecution of any foreign intelligence crime or crime that is inextricably linked with foreign intelligence.[194] In essence, the court gives prosecutors a choice in these cases between pursuing surveillance via the traditional Title III procedures, or opting for the different FISA procedures.

1. FISA Procedures Are Not as Protective of Individual Rights as Title III When the Government's Objective Is Criminal Prosecution

The expansion of FISA surveillance for use by prosecutors is troubling because, while FISA still requires probable cause, particularity, and issuance by a neutral magistrate, these requirements are specifically tailored to provide justification for intelligence surveillance and bear little relation to the type of justification traditionally required in criminal investigations.

a. Probable Cause

Probable cause exists when the facts and circumstances within government officials' knowledge through reasonably trustworthy information are sufficient in themselves to allow a person of reasonable caution to believe that certain circumstances exist.[195] The probable cause requirement protects privacy by requiring objective, verifiable justification for an intrusion, but it also protects the government's interests by creating a lower standard of proof to authorize intrusive investigation than would be required for a conviction.[196]

Title III authorizes electronic surveillance if "there is probable cause for belief that an individual is committing, has committed, or is about to commit" a specified criminal offense.[197] Under this standard, the intrusion into a person's privacy is justified by a link to criminal activity. In contrast, FISA requires probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power.[198] "Agent of a foreign power" includes, among

---

[194] *See supra* Part V.B (discussing primary purpose test under FISA).

[195] Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (quoting Carroll v. United States, 267 U.S. 132, 162 (1925)).

[196] *Brinegar*, 338 U.S. at 176.

[197] 18 U.S.C. § 2518(3)(a) (2000).

[198] 50 U.S.C. § 1805(a)(3)(A) (2000).

others, any person who "knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States . . . ."[199]

The difference between FISA and Title III is obvious. FISA requires no actual connection to criminal activity, and in its place requires probable cause to believe that the target of the surveillance is working on behalf of a foreign power, "which activities . . . may involve" criminal violations. This standard invites virtually unlimited surveillance based on flimsy connections to foreign activities which may or may not be crimes. This standard is barely sufficient to justify foreign intelligence gathering, much less criminal investigation, because it does not require the government to establish any likelihood that evidence of a crime or a threat to national security will be found.

b. Particularity

Under the Fourth Amendment, a warrant must particularly describe the place to be searched and the person or things to be seized.[200] This requirement serves to prevent general warrants.[201] It ensures that the scope of the search is "carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[202]

Title III requires probable cause to believe that "particular communications" concerning the specified offense will be obtained through the surveillance and also that the facility subject to surveillance is being used in connection with the crime.[203] FISA requires certification by a high level executive official that the information sought is foreign intelligence information and 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."[204]

Aside from the problem of trusting the "certification" of a government official, this requirement assures only that the communications being intercepted have some relation to the individual who is targeted. The statute does not limit the surveillance based on the content of the conversations. When the purpose of the surveillance is not merely intelligence gathering, but evidence gathering for purposes of criminal prosecution, the statute places immense power in the hands of law enforcement to intrude on that individual's privacy.

c. Neutral Magistrate

FISA strictly limits the magistrate's powers to review FISA applications. For example, FISC judges may not review the government's certification that the purpose of the surveillance is to obtain foreign intelligence information unless the surveillance involves a U.S. citizen, in which case the review is

---

199 *Id*. § 1801(b)(2)(A) (2000).
200 Maryland v. Garrison, 480 U.S. 79, 84 (1987).
201 *Id*.
202 *Id*.
203 18 U.S.C. §§ 2518(3)(b), (d) (2000).
204 50 U.S.C. §§ 1804(a)(7)(A), (4)(B) (2000).

limited to clear error. This certification is a key component of the FISA application because the connection to foreign intelligence provides the constitutional grounds for the limited procedures. Allowing executive self-regulation of this component severely limits the magistrate's ability to review the justification for the order.

The FISC judge's level of involvement in the FISA application is clearly lower than the level of involvement provided in Title III.[205] In the realm of foreign intelligence, it is appropriate for courts to defer to the discretion of the executive to some degree. However, the same degree of deference becomes dangerous in criminal investigations, even when those investigations involve foreign intelligence crimes, because it limits the judge's ability to act as a buffer between executive zeal and individual privacy.

As a whole, the FISA requirements of probable cause, particularity, and issuance by a neutral magistrate are minimal. By allowing the government to use these procedures in criminal investigations, *In re Sealed Case* authorized a significant expansion of the government's ability to invade individual privacy. The government will now be able to choose the FISA standards over the Title III standards to achieve prosecutorial objectives in a wide range of situations.

2. FISA Proceedings Are Conducted Ex Parte and Include a Significant Element of Self-Regulation by the Executive Branch, Presenting a Greater Opportunity for Abuse

The government's expanded ability to conduct FISA surveillance in situations involving "foreign intelligence crimes" and "ordinary crimes" related to foreign intelligence presents a greater risk of abuse than if the government were constrained to follow Title III procedures.

First, the FISA procedures provide significant deference to executive self-regulation because they prohibit review of the executive certification of purpose.[206] Given the significance of the purpose requirement, the fact that this certification is effectively non-reviewable leaves the executive in the position of defining the constitutional limits of its own behavior: "The power to define threats to the 'national security' is the power to draw the limits of acceptable behavior for leaders abroad and citizens at home."[207] The danger of this type of self-regulation is well documented.[208]

In fact, Congress enacted FISA in order to curb executive abuse of unregulated surveillance, but the enactment of FISA has not prevented abuse. In September 2000, for example, the DOJ voluntarily disclosed the fact that it had made errors in over seventy-five FISA applications.[209] Some of the errors

[205] *Compare* 50 U.S.C. § 1805 (2000) *with* 18 U.S.C. § 2518.

[206] Except to review for clear error when the target of the surveillance is a U.S. person. 50 U.S.C. § 1805(a)(5).

[207] MORTON H. HALPERIN ET AL., THE LAWLESS STATE: THE CRIMES OF THE U.S. INTELLIGENCE AGENCIES 5 (1976).

[208] *See, e.g.*, CHURCH COMMITTEE REPORT, BOOK II, *supra* note 13, at 14 (attributing executive abuse of unregulated surveillance to the lack of accountability and control normally provided by a system of checks and balances between branches).

[209] *In re All Matters*, 262 F. Supp. 611, 620 (FISA Ct. 2002).

involved misstatements or material omissions, while others involved intentional concealment of unlawful communications between the FBI and prosecutors that would have rendered the surveillances unconstitutional.[210] Another vibrant example was the revelation in late 2005 of a program of secret surveillance conducted by the National Security Agency completely outside of the FISA regime.[211] President Bush claimed to be justified in ordering and overseeing such surveillance because, "decisions made are made understanding we have an obligation to protect the civil liberties of the American people."[212] Because it leaves so much power in the hands of executive discretion, the use of FISA surveillance should not be expanded into the criminal realm where Title III procedures already operate.

Another aspect of FISA that presents a risk of abuse is the fact that FISA surveillance is conducted completely ex parte, with limited opportunity for challenge in an adversarial proceeding. Under FISA, the government need not disclose the fact that it has conducted surveillance unless it charges an individual with a crime.[213] Innocent parties whose conversations were intercepted by the government have no relief. Furthermore, a defendant who is prosecuted based on information gained in FISA surveillance does not have a right to access the original FISA application or order when the Attorney General claims that disclosure would harm national security.[214] Without access to the original application, the defendant's ability to challenge the legality of the surveillance is limited.

It is true that FISA offers other checks on unfettered executive discretion,[215] but those checks have proven unable to protect against abuse. The risk is even greater now that FISA surveillance may expand into the realm of criminal prosecution.

B. The FISCR's Use of the Special Needs Doctrine Presents the Danger of Expanding That Doctrine to Engulf the Warrant Requirement

The FISCR's interpretation and application of the special needs doctrine also raises Fourth Amendment concerns. The special needs doctrine generally applies to brief, warrantless searches or seizures conducted without individualized suspicion based on a special government need.[216] For example,

---

[210] *Id*.

[211] *Official: Bush Authorized Spying Multiple Times*, MSNBC.COM, Dec. 16, 2005, http://www.msnbc.msn.com/id/10488458 [hereinafter *Authorized Spying*].

[212] *Id*.

[213] 50 U.S.C. § 1806(c) (2000).

[214] *Id*. § 1806(f).

[215] *See* 50 U.S.C. § 1807 (2000) (requiring the Attorney General to submit a report to the courts and to Congress detailing the number of FISA applications submitted and whether those applications were granted, modified, or denied); 50 U.S.C. § 1808 (2000) (requiring a semiannual report to the House and Senate intelligence committees detailing each criminal case where evidence obtained by FISA surveillance was used at trial).

[216] Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990); City of Indianapolis v. Edmond, 531 U.S. 32 (2000); Illinois v. Lidster, 540 U.S. 419 (2003).

the Supreme Court has recognized roadblocks conducted to protect highway safety from the dangers of drunk driving as serving a special need,[217] as well as border searches to regulate persons entering the country.[218] Once the Court identifies a special need beyond the normal need of law enforcement, it will uphold the suspicionless and warrantless searches or seizures as long as the intrusion authorized is reasonable in relation to the government interest served.[219] The primary point of contention in special needs cases usually involves determining whether the government's interest qualifies as a special need.

In *City of Indianapolis v. Edmond*,[220] the Supreme Court held that a special need must be a hazard that goes beyond the government's "general interest in crime control," regardless of the gravity of the threat.[221] Applying this definition to a narcotics checkpoint conducted for the purpose of interdicting illegal drugs and prosecuting offenders, the Court held that the narcotics checkpoint did not qualify as a special need because it was conducted to serve a general law enforcement purpose.[222] In contrast, programs that serve a special need may incidentally result in the gathering evidence for criminal prosecution, but they must serve a programmatic purpose beyond general law enforcement.[223]

Applying this test to national security surveillance under FISA, the FISCR held that it qualifies as a special need because its purpose is to protect against a specific hazard, namely foreign intelligence crimes.[224] Gathering evidence for use in criminal prosecution is merely an incidental aspect of the programmatic purpose.[225]

The FISCR's interpretation of the special needs doctrine, in essence, allows the government to conduct warrantless surveillance to gain evidence of crimes so long as the government's programmatic purpose is something beyond general law enforcement. This rationale, if expanded, could just as easily justify surveillance to protect citizens from the dangers of organized crime, illegal possession of firearms, or other serious crimes. Warrantless surveillance targeted at stopping this type of crime would certainly alleviate a serious societal harm, but would also incidentally result in gathering evidence for criminal prosecution. This rationale, if widely accepted, would circumvent the warrant requirement altogether. Procedures in all government investigations would be governed by the general standard of reasonableness applied to national security surveillance.

---

[217] *Sitz*, 496 U.S. at 450.
[218] United States v. Martinez-Fuerte, 428 U.S. 543, 556–57 (1976).
[219] *Lidster*, 540 U.S. at 423.
[220] 531 U.S. 32 (2000).
[221] *Id*. at 41–42.
[222] *Id*. at 44.
[223] *Id*. at 46–47.
[224] *In re Sealed Case*, 310 F.3d, 717, 746 (FISA Ct.Rev. 2002).
[225] *Id*.

Furthermore, by classifying national security surveillance as serving a special need, the FISCR decision may result in "national security" becoming a shibboleth, the invocation of which provides the government special allowance to violate traditional civil liberties. The results of this decision may extend beyond the specific use of FISA surveillance and could infect the entirety of Fourth Amendment jurisprudence.

C. The In re Sealed Case *Decision Violated the Fourth Amendment Because It Authorized Government Surveillance That Is Unreasonable*

In re Sealed Case cannot be viewed in isolation. It must be viewed in light of the history of the Fourth Amendment and the history of national security surveillance. The FISCR opinion, in one light, merely adds another view to the long-standing argument articulated by Justices White and Douglas in their concurrences to *Katz*, as to whether executive self-regulation sufficiently prevents violations of Americans' civil liberties. On the one hand, some deference should be given to the executive branch to conduct national security surveillance without the full strictures of the ordinary criminal investigation warrant requirement, as Justice White argued. On the other hand, this exemption must not be so broad as to constitute a green light for executive abuse, as Justice Douglas warned, particularly given the executive's history of taking such freedom to the extremes and abusing both First and Fourth Amendment interests.

The FISCR opinion did not strike the appropriate balance. The opinion would unduly expand the use of self-regulated executive surveillance with limited opportunity for judicial review or adversarial testing. This expansion invites executive abuse and does not appropriately safeguard individual privacy. Furthermore, the FISCR's use of the special needs doctrine to create a national security exemption could be applied in future decisions to undermine the warrant requirement in other areas as well. In light of these concerns, the decision violated the Fourth Amendment because it authorizes government surveillance that is unreasonable.

VII. CONCLUSION

From the invention of wiretapping to the present, the status of national security surveillance under the Fourth Amendment has never been clear. It is clear, however, that national security surveillance presents a novel question, not comparable to any other type of government action. As the Supreme Court stated in *Keith*, national security surveillance presents an area where First and Fourth Amendment values converge.[226] The stakes, for both the government and for individual rights, are high. The application of the warrant requirement, the exact definition of probable cause, particularity, and issuance by a neutral magistrate all take on new meaning when applied to national security surveillance. The one word of the Fourth Amendment that applies as clearly to

[226] 407 U.S. 297, 314 (1972).

national security surveillance as to any other type of government intrusion is that it must be "reasonable."

In re Sealed Case failed to strike the appropriate balance between legitimate government needs and individual privacy when it expanded the use of FISA surveillance because it would result in degradation of individual privacy and unlimited executive power. However, the FISA regime need not be discarded entirely. FISA surveillance can meet the standard of "reasonableness" if sufficient safeguards are established to (1) allow a greater level of judicial review and opportunity for adversarial testing; and (2) ensure that the government may not use FISA as an end run around traditional warrant requirements.

The first safeguard can be met by amending FISA to allow expanded judicial review of the purpose of the surveillance. For example, the court should be required to find probable cause that foreign intelligence information will be found. This provision will not unduly burden the president's ability to conduct national security surveillance because, as stated in *Keith*, security matters are not too subtle or complex for judicial evaluation.[227] Further, Congress should require the government to give targets of FISA surveillance notice that the surveillance occurred. Congress can limit the adverse affects of requiring notice by allowing a buffer period between the end of the surveillance and the date notice is required, as well as by allowing an exception when disclosure would substantially prejudice national security.

The second safeguard presents a more difficult question since any restrictions Congress places on the use of FISA procedures present the risk of hampering the executive's ability to investigate foreign intelligence crimes. One possible remedy would be to list the type of crimes that may be investigated under FISA, such as terrorism, espionage, and sabotage by a foreign power or its agent. This type of listing would eliminate the uncertainty that resulted from the primary purpose test and that led to the formation of the Wall, but it would also accommodate the government's need for less strict procedures in certain criminal investigations involving foreign intelligence crimes.

With careful consideration, the legitimate needs of the government to protect the country from attack and overthrow can be balanced against individuals' "right to be let alone" from government intrusion. National security surveillance hinges on striking the appropriate Fourth Amendment's balance of "reasonableness" to ensure that neither interest is sacrificed in the name of the other.

---

[227] *Id*. at 320.