

ARTICLE

FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security

Scott J. Glick*

Abstract

In 2006, Congress enacted two potentially significant restrictions on the government's ability to collect foreign intelligence information pursuant to FISA. Against the backdrop of a Foreign Intelligence Surveillance Court of Review (Court of Review) decision that arguably reached an erroneous conclusion about the meaning and scope of FISA's significant purpose requirement, Congress let stand two restrictions that the Court of Review had placed on the government's use of FISA. First, the Court of Review held that if the government's primary purpose was to prosecute, then the government could use FISA only if it intended to prosecute an alleged terrorist or spy for what the court called a "foreign intelligence crime." The Court of Review also held that the government could not use FISA, even when it intended to prosecute for a foreign intelligence crime, if that crime occurred in the "past." This Article examines the Court of Review's decision and argues that the court reached an erroneous conclusion in

* Deputy Chief, Counterterrorism Section, National Security Division, U.S. Department of Justice; former Deputy Counsel for Criminal Matters, Office of Intelligence Policy and Review, U.S. Department of Justice. This article has been reviewed for publication by the Justice Department in accordance with 28 C.F.R. § 17.18. The views expressed in this article are solely those of the author and do not necessarily reflect the views of the Justice Department. The author wishes to thank Lisa Farabee, Daniel Marcus, David Rosenberg, and Richard Seamon for their review and comments on an earlier draft of this Article. The author also wishes to thank Dena Roth, J.D. Georgetown 2010, for her research assistance and comments.

regard to the scope of the government's power. The Article also takes a comprehensive and fresh look at the legislative history of FISA's purpose requirement, both before and after the Court of Review's decision. The Article demonstrates that Congress was keenly aware of the restrictions placed on the government by the Court of Review, and rather than explicitly expressing its will in a Final Conference Report with respect to that decision, it simply voted to repeal the amendment's sunset provision. The Article concludes by proposing legislation that would remove both of the restrictions placed on the government by the Court of Review.

Table of Contents

| | |
|---|-----|
| I. Introduction | 88 |
| II. Foreign Intelligence Collection in the United States | 92 |
| A. <i>From Olmstead to Keith</i> | 92 |
| B. <i>FISA</i> | 98 |
| III. FISA's Purpose Requirement | 102 |
| A. <i>The Primary Purpose Test and the FISA "Wall"</i> | 102 |
| B. <i>The Significant Purpose Requirement</i> | 111 |
| IV. And the Wall Came Tumbling Down | 116 |
| A. <i>The Decision by the FISC</i> | 116 |
| B. <i>Congressional Reaction to the FISC's Decision</i> | 117 |
| C. <i>The Decision by the Court of Review</i> | 120 |
| V. Repeal of the Sunset Provision | 124 |
| A. <i>The 2003 and 2004 Hearings</i> | 124 |
| B. <i>The 2005 Hearings</i> | 127 |
| C. <i>The Senate Bill and the House Bill</i> | 132 |
| D. <i>Final Debate and Passage of the Reauthorization Act</i> | 135 |
| VI. A Legislative Alternative | 137 |
| VII. Conclusion | 142 |

I. Introduction

Six weeks after the tragic events of September 11, 2001, then-Attorney General John Ashcroft gave a speech at the Emergency, Safety and Security Summit hosted by the U.S. Conference of Mayors. In his speech, Ashcroft echoed the aggressive approach that Robert Kennedy's Justice Department was said to have taken against "mobsters" who were

arrested for “spitting on the sidewalk” and stated that the American people faced a “serious, immediate and ongoing threat from terrorism.”¹ In Ashcroft’s view, history’s judgment would be “harsh” if the government failed to use “every available resource to prevent future terrorist attacks.” He promised that the Justice Department would “use all our weapons within the law and under the Constitution to protect life and enhance security for America.”²

The next day, on October 26, 2001, President Bush signed the USA PATRIOT Act³ into law, which dramatically altered the government’s ability to use the Foreign Intelligence Surveillance Act (FISA) of 1978⁴ against alleged terrorists and spies. As enacted in 1978, FISA permitted the government to obtain a court order from the Foreign Intelligence Surveillance Court⁵ (FISC) to conduct electronic surveillance to obtain foreign intelligence information from foreign powers and agents of foreign powers. Although Congress had amended FISA on numerous occasions between 1978 and October 2001 to permit the government to conduct physical searches,⁶ to obtain pen register and trap and trace data,⁷ and to obtain business records,⁸ arguably the most sweeping and controversial change to FISA came in October 2001 with Section 218 of the PATRIOT

¹ John Ashcroft, Att’y Gen., Prepared Remarks for the U.S. Mayors Conference (Oct. 25, 2001), *available at*

http://www.usdoj.gov/archive/ag/speeches/2001/agcrisisremarks10_25.htm.

² *Id.*

³ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 [hereinafter PATRIOT Act]. For a summary of the PATRIOT Act, *see* CHARLES DOYLE, THE USA PATRIOT ACT: A LEGAL ANALYSIS, CONG. RESEARCH SERV. RL 31377 (2002), *available at* <http://www.fas.org/irp/crs/RL31377.pdf>.

⁴ Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1811 (2006)) [hereinafter FISA].

⁵ The Foreign Intelligence Surveillance Court is a special Article III court created by FISA and is composed of the same Article III judges who serve as United States District Court judges. 50 U.S.C. § 1803(a) (2006).

⁶ Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443 (1994) (codified at 50 U.S.C. §§ 1821–1829 (2006)).

⁷ Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601(2), 112 Stat. 2396, 2404–05 (1998) (codified at 50 U.S.C. §§ 1841–1845 (2006)). A pen register device records data concerning *outgoing* telephone calls, and a trap and trace device records data concerning *incoming* telephone calls.

⁸ Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2410–11 (1998) (codified at 50 U.S.C. §§ 1861–1862 (2006)).

Act.⁹ Before passage of Section 218, the government had used Title III of the Omnibus Crime Control and Safe Streets Act of 1968,¹⁰ rather than FISA, when its primary purpose in seeking surveillance was to enforce the criminal law. After the PATRIOT Act was enacted, however, the government explicitly took the position that it could use FISA even if its primary purpose was to prosecute¹¹ because the amended FISA only required the government to certify that “a significant purpose” of the FISA collection was to obtain foreign intelligence information.¹²

Nine months after the PATRIOT Act was enacted, the FISC issued an order preventing government prosecutors from using FISA primarily to obtain evidence for a criminal prosecution.¹³ The government appealed, and, in November 2002, the special Article III appellate court set up by Congress to hear appeals from the FISC — the Foreign Intelligence Surveillance Court of Review¹⁴ — reversed the decision of the FISC and held that the government could use FISA to obtain evidence for a criminal prosecution.¹⁵ However, the Court of Review placed limitations on the government. Specifically, the Court of Review held that if the government’s primary purpose was to prosecute, then it could only use FISA if it intended to prosecute the alleged terrorist or spy for what it called a “foreign intelligence crime”.¹⁶ As a result, the Court of Review concluded that the government could not use FISA if the government intended to prosecute for an “ordinary” crime, even if that was the only way to protect national security, unless the ordinary crime was “inextricably intertwined” with a

⁹ See Peter P. Swire, *The System of Foreign Intelligence Law*, 72 GEO. WASH. L. REV. 1306, 1327 (2004). See also H.R. REP. NO. 109-174, pt. I, at 444 (2005), 2005 WL 1705108 (Dissenting Views) (reporting that by 2002, “389 communities and seven states ha[d] passed resolutions opposing parts of the PATRIOT Act”). See generally Susan N. Herman, *The USA PATRIOT Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.C.L. L. REV. 67 (2006) (same, and referencing a “grass roots movement”).

¹⁰ Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 212–223 (codified as amended at 18 U.S.C. §§ 2510–2520 (2006)) [hereinafter Title III].

¹¹ See Brief for the United States at 13–14, *In re* [deleted], No. 02-001, (FISA Ct. Rev. Aug. 21, 2002) (redacted version), available at <http://www.fas.org/irp/agency/doj/fisa/082102appeal.html>.

¹² PATRIOT Act § 218 (codified at 50 U.S.C. § 1804(a)(6)(B) (2006)).

¹³ See *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 613 (FISA Ct. 2002).

¹⁴ The Foreign Intelligence Surveillance Court of Review (Court of Review) was created by Congress in 1978. See 50 U.S.C. § 1803(b) (2006).

¹⁵ *In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002).

¹⁶ *Id.* at 735–41.

“foreign intelligence crime”.¹⁷ Moreover, the Court of Review held that the government could not use FISA, even when it intended to prosecute for a foreign intelligence crime, if its “sole objective” was to collect evidence of “past criminal conduct”.¹⁸

FISA never contained any provision that restricted the government’s use of it to only certain types of crimes, and, moreover, the terms “foreign intelligence crime” or “ordinary crime” were not terms that Congress had defined in FISA or anywhere else in the U.S. Code. Thus, the government had argued that it could use FISA to obtain evidence for a prosecution of an agent of a foreign power, regardless of the nature of the crime.¹⁹ The Court of Review disagreed, however, and concluded that Congress did not intend to give that power to the Executive Branch.²⁰ The government did not appeal the decision of the Court of Review, and, in subsequent hearings concerning section 218’s “sunset” provision,²¹ it indicated to Congress that no further changes to the significant purpose requirement were necessary. In March 2006, Congress passed the USA PATRIOT Improvement and Reauthorization Act of 2005, which permanently enacted section 218 into law without any changes to the section’s language or an explicit expression of Congress’s will in a Final Conference Report with respect to the Court of Review’s decision.²²

The purpose of this Article is to examine the Court of Review’s decision, to take a fresh look at the legislative history of FISA’s purpose requirement, and to propose legislation to remove both of the restrictions placed on the government by the Court of Review. This Article agrees with other legal scholars who have stated that the significant purpose amendment is constitutional, regardless of the type and nature of the crime that the government intends to prosecute, provided both that a significant purpose of the FISA collection is to obtain “protective” foreign intelligence

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ Supplemental Brief for the United States at 22, *In re* [deleted], No. 02-001 (FISA Ct. Rev. Sept. 25, 2002), available at <http://www.fas.org/irp/agency/doj/fisa/092502sup.html>.

²⁰ *In re Sealed Case*, 310 F.3d at 736.

²¹ The term “sunset” generally refers to a statute or regulation that terminates or expires after a specific period of time. When the PATRIOT Act was enacted, sixteen provisions, including the significant purpose amendment, were scheduled to expire on December 31, 2005. See PATRIOT Act § 224.

²² See USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 102, 120 Stat. 192, 195 (2006) [hereinafter Reauthorization Act].

information and that the other requirements of the statute have been met.²³ This Article also conclusively demonstrates congressional awareness of the Court of Review's decision and the limitations that were placed on the government. Although Congress missed a legislative opportunity to explicitly express its will, its reenactment of the significant purpose amendment, its rejection of an alternative proposal to expand government power, and the permanent elimination of the sunset provision should be presumed by the judiciary to be congressional endorsement of the limitations the Court of Review placed on the scope of the government's power.

As background for this Article, Part II briefly examines the history of foreign intelligence collection in the United States prior to FISA and provides an overview of FISA itself. Part III then provides a backdrop for an analysis of the Court of Review's decision by examining the "primary purpose" test, the FISA "wall" that had been erected between intelligence officers and prosecutors, and the initial passage of the significant purpose amendment. Part IV then looks at the intelligence sharing procedures promulgated by Attorney General Ashcroft to implement the significant purpose amendment, which led to the decisions by the FISC and the Court of Review. Thereafter, Part V closely examines the congressional hearings and debate that took place after the Court of Review's decision. Part VI argues that the Court of Review reached an erroneous conclusion in regard to the scope of the government's power and suggests a legislative alternative that would remove both of the restrictions placed on the government by the Court of Review. Part VI therefore recommends that Congress adopt a provision in FISA, similar to the one that Congress has adopted for Title III surveillances, that would add a new provision specifically authorizing the government to use FISA when a significant purpose of the collection is to obtain protective foreign intelligence information, regardless of the nature of the crime it intends to pursue.

II. Foreign Intelligence Collection in the United States

A. *From Olmstead to Keith*

Although "every President since Franklin D. Roosevelt has asserted the authority to authorize warrantless electronic surveillance" for foreign

²³ See *infra* notes 70–72 and accompanying text, which distinguish between "protective" foreign intelligence information and "positive" foreign intelligence information.

intelligence purposes,²⁴ it was not until Congress enacted FISA in 1978 that a comprehensive “statutory procedure” existed to enable federal officers, acting through the Attorney General, to obtain a judicial order authorizing the use of electronic surveillance in the United States for “foreign intelligence purposes.”²⁵ Prior to FISA, Congress had sought to regulate electronic surveillance by the Executive Branch on two occasions. The first was in 1934 in response to a decision by the Supreme Court in *Olmstead v. United States*.²⁶ In the *Olmstead* case, the Supreme Court held that the Fourth Amendment²⁷ did not prohibit wiretapping by the government unless it was accompanied by a physical trespass of the suspect’s property.²⁸ As a result, also in 1934, Congress enacted the Federal Communications Act, which made it a crime for any person “to intercept and divulge or publish the contents of wire and radio communications.”²⁹ In reviewing that statute in *Nardone v. United States*,³⁰ the Supreme Court first held that the statute applied to federal agents. When the case returned to the Court two years

²⁴ S. REP. NO. 95-604, pt. 1, at 7 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908–09 [hereinafter 1978 Senate Judiciary Committee Report]. See H.R. REP. NO. 95-1283, pt. 1, at 15–16 (1978) [hereinafter 1978 House Intelligence Committee Report]. On May 21, 1940, President Roosevelt wrote a letter to Robert H. Jackson, then Attorney General of the United States, stating that electronic surveillance would be proper under the Constitution where “grave matters involving the defense of the nation” were involved. Letter from Franklin D. Roosevelt, President of the United States, to Robert H. Jackson, Att’y Gen. (May 21, 1940), *reprinted in* ROBERT J. LAMPHERE & TOM SHACHTMAN, *THE FBI-KGB WAR: A SPECIAL AGENT’S STORY* 102 (1986). See generally William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1–25 (2000).

²⁵ 1978 Senate Judiciary Committee Report, *supra* note 24, at 5 (“The purpose of the bill is to provide a procedure under which the Attorney General can obtain a judicial warrant authorizing the use of electronic surveillance in the United States for foreign intelligence purposes.”).

²⁶ 277 U.S. 438 (1928). *Olmstead* and a number of other individuals were convicted of conspiracy to violate the National Prohibition Act by unlawfully possessing, transporting, and importing intoxicating liquors. The wiretap evidence was obtained by federal prohibition officers who intercepted telephone communications at the suspects’ residences and their business “without trespass on any property of the defendants.” *Id.* at 457.

²⁷ The Fourth Amendment to the United States Constitution provides that “[t]he right of the people to be secure in their persons . . . against unreasonable searches and seizures, shall not be violated”, and the warrant clause requires that “no Warrants shall issue, but upon probable cause . . . particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV.

²⁸ *Olmstead*, 277 U.S. at 464–66.

²⁹ The Federal Communications Act of 1934, ch. 652, 48 Stat. 1103 (codified as amended at 47 U.S.C. § 605 (2006)).

³⁰ 302 U.S. 379, 384 (1937).

later, the Court held that if the statute were violated, any information or evidence derived from those interceptions would be inadmissible in court.³¹ The Justice Department, however, did not interpret the 1934 Act or the *Nardone* decisions as prohibiting, “per se”, warrantless electronic surveillance for foreign intelligence purposes.³² Rather, “only the interception *and* divulgence of their contents outside the Federal establishment was considered to be unlawful. Thus, the Justice Department found continued authority for its national security wiretaps.”³³

Consequently, the FBI continued to conduct electronic surveillance in matters relating to national security. Indeed, the Justice Department publicly stated its policy in regard to a foreign intelligence exception in a 1966 supplemental brief to the Supreme Court in the case *Black v. United States*.³⁴ In its brief, the Department stated that “present department practice” for the “entire Federal establishment” prohibits the use of microphones, and other listening devices that can intercept telephone and other wire communications, “in all instances *other than* those involving the collection of intelligence affecting the national security. The specific authorization of the Attorney General must be obtained in each instance when this exception is invoked.”³⁵

In 1967, the Supreme Court overruled its holding in *Olmstead* on the extent of Fourth Amendment protection when it decided *Katz v. United States*.³⁶ In *Katz*, the Court held that the Fourth Amendment protects “people, not places”, and that it prohibited warrantless electronic surveillance even if there were no physical trespass.³⁷ In subsequent decisions, the Supreme Court generally adopted the “reasonable expectation of privacy” test articulated by Justice Harlan in his concurring opinion in *Katz*.³⁸ *Katz*, however, was an ordinary criminal case involving

³¹ *Nardone v. United States*, 308 U.S. 338, 341 (1939).

³² 1978 Senate Judiciary Committee Report, *supra* note 24, at 10.

³³ *Id.* (emphasis added).

³⁴ 1978 Senate Judiciary Committee Report, *supra* note 24, at 11.

³⁵ *Id.* at 12 (quoting the Solicitor General’s supplemental brief) (emphasis added).

³⁶ 389 U.S. 347 (1967).

³⁷ *Id.* at 351–53. In *Katz*, government agents attached an electronic device to the outside of a public telephone booth and recorded Katz while he was transmitting gambling information. *Id.* at 348.

³⁸ *Id.* at 360–61 (Harlan, J., concurring) (“My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”); *see generally* 1 Wayne R. LaFare, SEARCH

the transmission of wagering information by telephone from California to Florida and Massachusetts in violation of federal law, and the Supreme Court explicitly declined to extend its ruling to cases “involving national security”.³⁹

The second occasion when Congress sought to regulate electronic surveillance came in 1968 in response to the Supreme Court’s decision in *Katz*. One year after *Katz*, Congress passed Title III, which made it unlawful for the government to intercept wire or oral communications without a specific statutory exception.⁴⁰ In Title III, Congress required the government to follow a detailed statutory scheme to obtain a court order to conduct electronic surveillance for law enforcement purposes, and it only permitted the government to use Title III to obtain evidence of certain crimes.⁴¹ The 1968 Congress, however, disclaimed any intention to legislate in regard to a “national security” or “foreign intelligence” exception.⁴² Indeed, in Title III, Congress explicitly endorsed what had been the Executive Branch’s view concerning the Federal Communications Act of 1934 through the following caveat:

Nothing contained in this chapter or in section 605 of the Communications Act of 1934 . . . 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.⁴³

AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(b)–(d) (4th ed. 2004).

³⁹ *Katz*, 389 U.S. at 358 n.23.

⁴⁰ See Title III, 82 Stat. at 213 (codified as amended at 18 U.S.C. § 2511(1) (2006)) (“Except as otherwise specifically provided in this chapter” any person who intentionally intercepts wire, oral, or electronic communications is guilty of an offense.).

⁴¹ *Id.* at 214 (codified as amended at 18 U.S.C. § 2516 (2006)). See S. REP. NO. 90-1097, at 36 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2156. This provision of Title III has been amended on several occasions by Congress since 1968 to enable the government to use Title III to obtain evidence of numerous additional criminal offenses, including most recently in the Reauthorization Act.

⁴² See S. REP. NO. 90-1097, at 35–36 (noting the “need for comprehensive, fair and effective reform setting uniform standards”).

⁴³ Title III, 82 Stat. at 217, repealed by FISA § 201(c) (emphasis added). The scope of the President’s constitutional authority to conduct warrantless electronic surveillance is beyond the scope of this Article.

As a result, nothing in Title III inhibited the Executive Branch from continuing to intercept wire and oral communications on the basis of a “national security” or “foreign intelligence” exception to the Fourth Amendment. Against this backdrop, as well as the domestic turmoil associated with the opposition of numerous Americans to the Vietnam War and other policies of the government, the *Keith* case reached the Supreme Court.⁴⁴

The *Keith* case concerned electronic surveillance that was conducted by the government in connection with a plot to bomb a Central Intelligence Agency office in Ann Arbor, Michigan.⁴⁵ Although the government did not seek to use the fruits of the electronic surveillance against the defendants who were charged with conspiracy in that case, during the pretrial proceedings, the defendants moved the court to order the government to disclose whether electronic surveillance had taken place. The defendants also sought a hearing to determine whether any of the government’s evidence was “tainted”.⁴⁶ In response, the government submitted an affidavit from the Attorney General that stated that he had approved the wiretaps “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.”⁴⁷ The government argued that the surveillance was a reasonable exercise of the “President’s power (exercised through the Attorney General) to protect the national security.”⁴⁸ The District Court disagreed and held that the surveillance violated the Fourth Amendment.⁴⁹ The government then filed a writ of mandamus in the Court of Appeals for the Sixth Circuit. On appeal, the Sixth Circuit upheld the District Court’s ordered disclosure of the overheard conversation.⁵⁰

The Supreme Court affirmed the judgment of the Court of Appeals. The Court rejected the notion that “special circumstances” were applicable

⁴⁴ United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972). The case is known as the “*Keith*” case because the government filed a writ of mandamus against the Honorable Damon Keith, United States District Court Judge, when he ordered the government to disclose wiretapping information.

⁴⁵ *Id.*

⁴⁶ *Id.* at 299–300.

⁴⁷ *Id.* at 300.

⁴⁸ *Id.* at 301.

⁴⁹ *Id.*

⁵⁰ United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 301 (1972).

to domestic security surveillances and held that the government was required to obtain a warrant pursuant to Title III to obtain the content of the conversations.⁵¹ The Court weighed the government's asserted need against the level of intrusion and applicable Fourth Amendment principles and declined to find a domestic security exception to Title III's requirements.⁵² However, the *Keith* Court invited Congress to consider "protective standards" for domestic security that "differ from those already prescribed for specified crimes in Title III" because "domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.'"⁵³ The Court also observed that the "gathering of security intelligence is often long range and involves the interrelation of various sources and types of information."⁵⁴ Thus, the Court opined in dicta:

[d]ifferent standards 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.⁵⁵

Importantly, the Court also limited its ruling by expressly pointing out that the case involved "only the domestic aspects of national security. We have not addressed and express no opinion as to the issues which may be involved with respect to activities of foreign powers or their agents."⁵⁶ Indeed, in a footnote, the Court cited two lower court cases that found warrantless surveillance constitutional "where foreign powers are involved."⁵⁷

Keith was followed by decisions by Courts of Appeal for the Third, Fifth, and Ninth Circuits that found a "foreign intelligence" exception to the

⁵¹ *Id.* at 318–20.

⁵² *Id.*

⁵³ *Id.* at 322. As discussed in Part IV.C. *infra*, the Court of Review would later draw a distinction between "ordinary" crimes and "foreign intelligence" crimes.

⁵⁴ *Id.*

⁵⁵ *Id.* at 322–23 (emphasis added). Four years prior to its decision in *Keith*, the Supreme Court weighed the government's law enforcement needs as well as its interest in preventing crime and saving lives and found a "stop and frisk" exception to the Fourth Amendment's probable cause requirement. See *Terry v. Ohio*, 392 U.S. 1 (1968).

⁵⁶ *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 321–22 (1972).

⁵⁷ *Id.* at 322 n.20 (citing *United States v. Smith*, 321 F. Supp. 424, 425–26 (C.D. Cal. 1971) and *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970)).

Fourth Amendment's warrant requirement.⁵⁸ The Court of Appeals for the District of Columbia Circuit, however, stated in dicta that "absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional."⁵⁹ By 1978, after a series of hearings and proposed legislation, Congress established "different standards" for foreign intelligence collection. Congress concluded that the "different policy and practical considerations" involved in domestic security surveillance applied "with even greater force" to foreign intelligence collection involving foreign powers and agents of foreign powers.⁶⁰ As a result, when it finally passed FISA, Congress departed from Title III's requirements for court-authorized electronic surveillance for surveillance targeting foreign powers and agents of foreign powers.⁶¹

B. FISA

Enacted in the wake of the Watergate scandal and other revelations concerning Executive Branch abuses,⁶² FISA establishes a statutory procedure that permits the government to conduct electronic surveillance⁶³

⁵⁸ *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977).

⁵⁹ *Zweibon v. Mitchell*, 516 F.2d 594, 613–14 (D.C. Cir. 1975) (en banc). Then-Attorney General John Mitchell was sued by Zweibon and other individuals who alleged that there had been unlawful electronic surveillance of their organization's headquarters. *Id.* at 596. Some scholars believe that the dicta in *Zweibon* also "influenced the enactment of FISA." Richard H. Seamon & William D. Gardner, *The PATRIOT Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319, 334 (2005).

⁶⁰ S. REP. NO. 95-701, at 15 (1978), reprinted in 1978 U.S.C.C.A.N. 3973, 3984 [hereinafter 1978 Senate Intelligence Committee Report].

⁶¹ 1978 Senate Intelligence Committee Report, *supra* note 60, at 15 ("these departures from traditional Fourth Amendment criminal law enforcement standards are constitutional" and are "supported by the Supreme Court's opinion in the *Keith* case"); *see also* 1978 Senate Judiciary Committee Report, *supra* note 24, at 13–14.

⁶² The extensive investigations of the government's intelligence activities that were led by Senator Frank Church culminated in a seven-volume report. *See Intelligence Activities and the Rights of Americans*, Final Rep. of the Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities. S. REP. NO. 94-755 (1976), available at http://www.aarlibrary.org/publib/church/reports/book2/html/ChurchB2_0001a.htm.

⁶³ "Electronic surveillance" is a term of art in FISA that includes the "acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States." 50 U.S.C. § 1801(f)(1) (2006).

targeting foreign powers⁶⁴ and agents of foreign powers⁶⁵ to obtain “foreign intelligence information”.⁶⁶ In regard to a “United States person”, which includes U.S. citizens as well as aliens lawfully admitted for permanent residence,⁶⁷ FISA’s definition of an agent of a foreign power largely centers on criminal conduct. For example, the government may target a United States person if it establishes that the person knowingly engages in: (1) clandestine intelligence gathering activities on behalf of a foreign power, which involve or may involve a violation of the criminal statutes of the United States; (2) sabotage; or (3) international terrorism.⁶⁸ “[I]nternational terrorism” is defined as activities that “involve violent acts or acts dangerous to human life” and that violate criminal laws or “would be a criminal violation” if committed within the United States.⁶⁹

Foreign intelligence information that may be sought under FISA generally falls into two categories: protective foreign intelligence information and positive foreign intelligence information.⁷⁰ Protective foreign intelligence information generally refers to threat-related information that “relates to, and if it concerns a United States person is necessary to, the ability of the United States to protect against” one of the following three

⁶⁴ “Foreign power” is a term of art in FISA that includes “a foreign government or any component thereof, whether or not recognized by the United States.” 50 U.S.C. § 1801(a)(1) (2006).

⁶⁵ *Id.* § 1801(b).

⁶⁶ *Id.* § 1801(e); *id.* § 1802.

⁶⁷ *Id.* § 1801(i).

⁶⁸ *Id.* § 1801(b)(2). For non-United States persons, an agent of a foreign power includes any person who: (1) acts in the United States as an officer or employee of a foreign power; (2) acts on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person’s presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or (3) engages in the international proliferation of weapons of mass destruction or activities in preparation therefor. *Id.* § 1801(b)(1).

⁶⁹ *Id.* § 1801(c). In order to constitute “international terrorism” such activities must also appear to be intended to “intimidate or coerce a civilian population[,] to influence the policy of a government by intimidation or coercion[,] or to affect the conduct of a government by assassination or kidnapping,” and they must occur “totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.” *Id.*

⁷⁰ See Seamon & Gardner, *supra* note 59, at 343; David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL’Y REV. 487 n.57 (2006).

threats to national security: “(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism or the international proliferation of weapons of mass destruction 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”.⁷¹ Positive foreign intelligence information, on the other hand, is generally not tied to a specific threat or criminal event, but instead it refers to “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.”⁷²

Before foreign intelligence collection may begin pursuant to FISA, the government must establish each of the enumerated requirements of the statute. The government usually submits an application⁷³ that, among other things, contains a description, if known, of the specific target of the electronic surveillance⁷⁴ as well as the facts and circumstances supporting the belief that: (1) the target is a foreign power or an agent of a foreign power; and (2) the target uses or is about to use the targeted facility (e.g., a telephone).⁷⁵ In addition to these requirements, FISA also mandates that a high-ranking Executive Branch official with national security

⁷¹ 50 U.S.C. § 1801(e)(1) (2006).

⁷² *Id.* § 1801(e)(2). *See also In re Sealed Case*, 310 F.3d 717, 723 n.9 (FISA Ct. Rev. 2002).

⁷³ FISA contains an emergency provision that permits the government to begin surveillance as soon as the Attorney General determines that the factual basis for issuance of an order under FISA exists, provided that an application is submitted to the FISC within seven days. 50 U.S.C. § 1805(e)(1) (2006).

⁷⁴ The statutory requirements for an order authorizing a physical search pursuant to FISA are identical in all material respects to the requirements for an order authorizing electronic surveillance pursuant to FISA, the one major exception being that an application to conduct a physical search pursuant to FISA must also contain a statement of the facts and circumstances supporting probable cause to believe that “the premises or property to be searched contains foreign intelligence information.” *See id.* § 1823(a)(3)(B). The citations to FISA that appear in this Article, however, are only to the electronic surveillance provisions.

⁷⁵ *See id.* § 1804(a)(1)–(9) (setting forth the items required in an application for an electronic surveillance order pursuant to FISA).

responsibilities⁷⁶ certify that a “significant purpose”⁷⁷ of the surveillance is to obtain foreign intelligence information.⁷⁸

Following the Attorney General’s approval,⁷⁹ the FISA application is submitted to the FISC: a “detached and neutral body.”⁸⁰ Before the FISC may approve the requested surveillance, however, the FISA judge must find that the application contains all of the statements and certifications required by the statute, including that there is probable cause to believe that the target is a foreign power or an agent of a foreign power and that the target uses or is about to use the targeted facility.⁸¹ Finally, FISA permits the use of information obtained and derived from any lawful electronic surveillance in criminal (as well as non-criminal) proceedings as long as the use comports with FISA’s requirements.⁸²

The foregoing overview of FISA demonstrates that Congress set forth a detailed statutory scheme that regulates the Executive Branch’s ability to conduct electronic surveillance targeting foreign powers and agents of foreign powers, and the amended FISA permits the government to obtain a court order when a significant purpose of that surveillance is to obtain foreign intelligence information. As discussed in Part IV, the Court of Review would later conclude that if obtaining foreign intelligence information is a “significant purpose” of the FISA collection, then the primary purpose could be to obtain evidence of a criminal offense.⁸³ The

⁷⁶ *Id.* § 1804(a)(6).

⁷⁷ Prior to the passage of the PATRIOT Act, the certifying official was required to state that “the purpose” of the surveillance was to obtain foreign intelligence information. *See infra* note 98 and accompanying text.

⁷⁸ 50 U.S.C. § 1804(a)(6)(B) (2006). *See generally id.* § 1804(a)(6)(A)–(E) (setting forth the required certifications by a high-ranking Executive Branch official with national security responsibilities).

⁷⁹ *See id.* § 1804(a).

⁸⁰ *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987).

⁸¹ 50 U.S.C. § 1805(a)(4) (2006); *see also supra* note 75. Although FISA is focused on the target’s status (e.g., an agent of a foreign power) and, in the case of a telephone, the target’s use of that telephone, and Title III requires the government to prove that the suspect is using the telephone to commit a crime (e.g., the so-called “dirty call”), the quantum of proof that is required — the probable cause — is the same under both statutes. *See, e.g., United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (the court must “make a practical, common-sense decision whether given all the circumstances set forth in the affidavit before [it] [that] there is a fair probability [that the target of the FISA collection] was an agent of a foreign power”) (internal citations omitted).

⁸² *See* 50 U.S.C. § 1806 (2006).

⁸³ *See In re Sealed Case*, 310 F.3d 717, 735 (FISA Ct. Rev. 2002).

statute itself, however, is silent on the type and nature of the crimes that the government may pursue when it seeks to use FISA. This silence is noteworthy particularly when contrasted with Title III, which enumerates the specific statutory predicates for which evidence may be sought.⁸⁴

III. FISA's Purpose Requirement

A. *The Primary Purpose Test and the FISA "Wall"*

To understand why Congress enacted the significant purpose amendment, this Part of the Article provides an overview of the "primary purpose" test and the FISA "wall". The word "wall" was used to describe the metaphorical barrier that existed between counterintelligence and law enforcement agents in the Executive Branch.⁸⁵ A number of legal commentators have recounted the history of the primary purpose test and the FISA wall, including its legal and cultural origins.⁸⁶ While this Article provides context for the actions taken by the legislative and judicial branches, it does not focus on the rise or fall of the wall, the people involved, or how the wall functioned. Rather, this Article focuses on the legislative history of the significant purpose amendment, the federal judiciary's reaction to that amendment, and the subsequent congressional reaction.

According to the Court of Review, the primary purpose test originated in the Fourth Circuit's decision in *United States v. Truong Dinh Hung*.⁸⁷ Truong was a Vietnamese citizen and son of a prominent Vietnamese politician who came to the United States in 1965.⁸⁸ Truong had met Dung Krall, a Vietnamese-American woman, and persuaded Krall to carry packages for him to the Vietnamese community in Paris at the time that negotiations were taking place between Vietnam and the United States.

⁸⁴ See *infra* note 312 and accompanying text.

⁸⁵ *In re Sealed Case*, 310 F.3d at 721.

⁸⁶ See e.g., William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma — A History*, 11 LEWIS & CLARK L. REV. 1099 (2007); Kris, *supra* note 70, at 487; Seamon & Gardner, *supra* note 59, at 423. One such article prominently identifies the names of Justice Department officials who played a role in the erection and fortification of the wall. Dianne C. Piette & Jesselyn Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall"*, 17 STAN. L. & POL'Y REV. 437 (2006).

⁸⁷ See *In re Sealed Case*, 310 F.3d at 725 (citing *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980)).

⁸⁸ *Truong*, 629 F.2d at 911.

The packages contained copies of “diplomatic cables and other classified papers of the United States government.”⁸⁹

Truong’s telephone and apartment were targeted with electronic and audio surveillance. No court authorization was obtained, however, before the surveillance was conducted. Thus, the electronic surveillance at issue was surveillance that was authorized by the Attorney General and not by any court.⁹⁰ The defendants were arrested and charged with conspiracy to commit espionage and several espionage-related offenses, and the fruits of the electronic surveillance were provided to them in discovery.⁹¹ The defendants argued that the evidence should be suppressed because the government’s investigation was “criminal” and it had failed to obtain a court order to conduct the surveillance. After reviewing several internal government memoranda and hearing testimony from certain government witnesses, including then-Attorney General Griffin Bell,⁹² the district court concluded that while the investigation may have commenced as a foreign intelligence investigation, at a certain point the investigation became “primarily criminal”. As a result, a warrant was required to conduct the surveillance.⁹³ Although the district court agreed with the government that a foreign intelligence exception to the warrant requirement existed, the district court also concluded that the government could proceed without a warrant “only so long as the investigation was ‘primarily’ a foreign intelligence investigation.”⁹⁴

The Court of Appeals for the Fourth Circuit agreed with the district court that a foreign intelligence exception to the Fourth Amendment’s warrant requirement existed. Citing the Supreme Court’s decision in *Keith*, the Court stated that the “needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, ‘unduly frustrate’ the President in carrying out his foreign affairs responsibilities.”⁹⁵ As a result of the “need of the executive branch for flexibility”, the Court of Appeals concluded that the federal courts should “not require the executive to secure

⁸⁹ *Id.*

⁹⁰ *Id.* at 912.

⁹¹ *Id.*

⁹² *Id.* at 916 n.5.

⁹³ *Id.* at 913.

⁹⁴ *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980).

⁹⁵ *Id.*

a warrant each time it conducts foreign intelligence surveillance.”⁹⁶ Instead, when the government conducts warrantless electronic surveillance targeting a “foreign power, its agent or collaborators”, such surveillance is permissible under the Fourth Amendment provided that the surveillance is conducted “primarily” for “foreign intelligence reasons”.⁹⁷ Although the Court of Appeals noted that prior to its opinion Congress had enacted FISA, the government’s surveillance activities pre-dated the enactment of FISA. Consequently, the analysis conducted by the Court of Appeals with respect to a foreign intelligence exception was a constitutional analysis, not a statutory analysis of whether FISA itself required a “primary purpose” test.

The text of FISA has never included the word “primary” in relation to the government’s purpose. Instead, FISA required the certifying official to state that “the purpose” of the electronic surveillance was to obtain foreign intelligence information.⁹⁸ Nonetheless, following *Truong*, many federal courts used the term “primary purpose” in describing the government’s conduct.⁹⁹ The Court of Appeals for the First Circuit stated that although evidence obtained under FISA “may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance.”¹⁰⁰ The Court of Appeals for the Eleventh Circuit also approved electronic surveillance conducted pursuant to FISA because the surveillance “did not have as its purpose the primary objective of investigating a criminal act.”¹⁰¹ The Ninth Circuit, however, refused to “draw too fine a distinction between criminal and intelligence investigations” and instead noted that, by “definition”, the term “international terrorism” “requires an investigation of activities that constitute crimes.”¹⁰²

In order to determine whether the government’s primary purpose in conducting the electronic surveillance was criminal or became criminal, the *Truong* court had relied on internal memoranda and testimony from

⁹⁶ *Id.* at 914.

⁹⁷ *Id.* at 915.

⁹⁸ FISA § 104(7)(B) (codified as amended at 50 U.S.C. § 1801(a)(7)(B) (2006)).

⁹⁹ *E.g.*, *United States v. Megahey*, 553 F. Supp. 1180 (E.D.N.Y. 1982), *aff’d sub nom.*, *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984); *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991).

¹⁰⁰ *United States v. Johnson*, 952 F.2d at 572.

¹⁰¹ *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987) (citations omitted).

¹⁰² *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988).

government witnesses, including the Attorney General.¹⁰³ After *Truong*, some Justice Department officials concluded that consultations and coordination among intelligence agents and law enforcement agents and prosecutors would become relevant to federal courts that might inquire into the purpose of the surveillance if FISA information were used as evidence in a criminal case.¹⁰⁴ Thus, some believed that the more consultations that occurred or the more that FISA was used to obtain evidence for a criminal prosecution, “the more likely courts were to find an improper purpose.”¹⁰⁵

In July 1995, then-Attorney General Janet Reno approved coordination procedures that “applied in most cases.”¹⁰⁶ The 1995 Coordination Procedures limited contacts between the FBI and the Criminal Division in cases where FISA collection was taking place in order to “avoid running afoul of the primary purpose test used by some courts.”¹⁰⁷ The procedures stated that the FBI and the Criminal Division should ensure that any advice that was given did not “inadvertently result in either the fact or the appearance of the Criminal Division’s directing or controlling” the intelligence investigation.¹⁰⁸ Later, in April 2002, the FISC amended its own internal rules and adopted Rule 11, which required that “all FISA applications” include “informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between FBI and criminal prosecutors at the Department of Justice or a United States Attorney’s Office.”¹⁰⁹ After reviewing the history associated

¹⁰³ *United States v. Truong Dinh Hung*, 629 F.2d 908, 916 (4th Cir. 1980).

¹⁰⁴ One internal DOJ memorandum stated that the “greater the involvement of prosecutors in the planning and execution of FISA searches, the greater is the chance that the government could not assert in good faith that the ‘primary purpose’ was the collection of foreign intelligence.” Kris, *supra* note 70, at 499 n.69 (citing Memorandum from Walter Dellinger, Assistant Att’y Gen. for the Office of Legal Counsel, on Standards for Searches Under the Foreign Intelligence Surveillance Act to Michael Vatis, Deputy Director, Executive Office for National Security (Feb. 14, 1995)).

¹⁰⁵ See Kris, *supra* note 70, at 498.

¹⁰⁶ *Id.* at 500.

¹⁰⁷ *In re Sealed Case*, 310 F.3d 717, 727 (FISA Ct. Rev. 2002).

¹⁰⁸ Memorandum from the Att’y Gen. to Assistant Att’y Gen. of the Criminal Division, the Director of the FBI, Counsel for Intelligence Policy and United States Attorneys, on Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations, Part A, ¶ 6 (July 19, 1995), available at <http://www.fas.org/irp/agency/doj/fisa/1995procs.html>.

¹⁰⁹ *In re Sealed Case*, 310 F.3d at 730. The Court of Review vacated this rule, and the current FISC rules have no such requirement. See Foreign Intelligence Surveillance Court Rules of Procedure (2006), available at http://www.uscourts.gov/rules/FISC_Final_Rules_Feb_2006.pdf.

with the Attorney General's 1995 Coordination Procedures, the Court of Review found that the "directing or controlling language" came to be "narrowly interpreted within the Department of Justice" to require that certain Justice Department officials act as a "wall" to prevent FBI intelligence officials from communicating with the Criminal Division in regard to ongoing foreign intelligence investigations and foreign counterintelligence investigations.¹¹⁰ Thus, the "foundations of the FISA wall lie in the 'primary purpose' test", and DOJ maintained the wall "influenced by its belief that the courts would require the wall if presented with the question."¹¹¹

The 1995 Coordination Procedures, however, simply fortified a natural separation that already existed between intelligence and criminal investigations at the time that FISA was enacted in 1978.¹¹² Indeed, it is not possible to review the entirety of the legislative history of FISA without coming to the conclusion that, in fact, an actual distinction existed at the time between intelligence investigations and purposes on the one hand and criminal investigations and law enforcement purposes on the other. For example, in 1976, in connection with predecessor legislation to FISA, then-Attorney General Edward Levi testified:

the bill's provisions necessarily reflect . . . the *distinct* national interest that foreign intelligence surveillances are intended to serve. *The primary purpose of such surveillances is not to obtain evidence for criminal prosecution although that may be the result in some cases.* The purpose, instead, is to obtain information concerning the actions of foreign powers and their agents in this country — information that may often be critical to the protection of the Nation from foreign threats.¹¹³

¹¹⁰ *In re Sealed Case*, 310 F.3d at 728 (citing DEP'T OF JUSTICE, FINAL REPORT OF THE ATTORNEY GENERAL'S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NATIONAL LABORATORY INVESTIGATIONS 721–34 (2000), [hereinafter BELLOWS REPORT], available at <http://www.usdoj.gov/ag/readingroom/bellows.htm>).

¹¹¹ Kris, *supra* note 70, at 499–500.

¹¹² See 1978 Senate Intelligence Committee Report, *supra* note 60, at 14 ("The differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities have been taken into account."); see Funk, *supra* note 86, at 1137 ("It had not generally been difficult to identify which surveillances were 'intelligence' surveillances and which were 'law enforcement' surveillances in previous years for a variety of historical and institutional reasons.").

¹¹³ *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearing Before the*

The four Congressional Reports most frequently cited as part of the legislative history of FISA — the Report by the House Permanent Select Committee on Intelligence,¹¹⁴ the Report by the Senate Judiciary Committee,¹¹⁵ the Report by the Senate Select Committee on Intelligence,¹¹⁶ and the Final House Conference Report¹¹⁷ — also contain evidence of the distinction that existed between the government’s investigative purposes. An examination of these Reports also reveals that, while a natural separation existed between intelligence and criminal purposes, this did not necessarily mean that FISA would never be used to gather evidence of a crime or that those purposes were mutually exclusive.

For example, the House Intelligence Committee wrote in its Report that “[n]othing in [FISA] relates to law enforcement procedures”¹¹⁸ and placing FISA in Title 18 would “wrongly suggest” that the “bill’s procedures deal with law enforcement.”¹¹⁹ The Report stated further that the “primary purpose of electronic surveillance pursuant to [FISA] is *not likely* to be the gathering of criminal evidence.”¹²⁰ Two other similar references are contained in the House Report.¹²¹

On the other hand, the House Intelligence Committee also stated in its Report that “[h]ow [FISA] information may be used ‘to protect’ against

Subcomm. on Intelligence and the Rights of Americans, S. Select Comm. on Intelligence, 94th Cong. 77 (1976) (statement of Att’y Gen. Edward Levi) (emphasis added). Legal scholars reviewing the history of the wall have also made this same observation. *See, e.g.*, Funk, *supra* note 86, at 1137 (“The intelligence/law enforcement dichotomy that underlay what the government sought to obtain in FISA was of long standing.”); Kris, *supra* note 70, at 496 n.62 (“Legally, this dichotomy goes back at least to the law enforcement proviso of the National Security Act of 1947, which prescribed the jurisdiction of the CIA and the FBI and prohibited the CIA from engaging in domestic law enforcement. . . . A culture of separation may have also developed because of the way the law developed . . . [and how] government wiretapping for intelligence purposes other than prosecution continued[]” after the Supreme Court’s decision in *Nardone*.).

¹¹⁴ *See supra* note 24.

¹¹⁵ *See supra* note 24.

¹¹⁶ *See supra* note 60.

¹¹⁷ H.R. REP. No. 95-1720, at 19 (1978) (Conf. Rep.), *reprinted in* 1978 U.S.C.C.A.N. 4048.

¹¹⁸ 1978 House Intelligence Committee Report, *supra* note 24, at 28.

¹¹⁹ *Id.*

¹²⁰ *Id.* at 89 (emphasis added).

¹²¹ *Id.* at 36 (“surveillance under this bill are *not primarily* for the purpose of gathering evidence of a crime”) (emphasis added); *id.* at 60 (FISA surveillances are “unlike” Title III surveillances, the “very purposes of which are to obtain evidence of criminal activity”). *See* 1978 Senate Intelligence Committee Report, *supra* note 60, at 41–42 (same).

clandestine intelligence activities *is not prescribed* by the definition of foreign intelligence information, although, of course, how it is used may be affected by minimization procedures.”¹²² The House Report then went on to state that “obviously” the use of foreign intelligence information that is “sought” by FISA could be used as “evidence in a criminal trial” and that this was:

one way the Government can lawfully *protect against* clandestine intelligence activities, sabotage, and international terrorism. The bill, therefore, explicitly recognizes that information which is evidence of crimes involving clandestine intelligence activities, sabotage, and international terrorism can be *sought*, retained, and used pursuant to this bill.¹²³

Moreover, the House Report stated that “evidence of certain crimes like espionage [and terrorism] would itself constitute ‘foreign intelligence information’ . . . because it is necessary to *protect against* [such activities] by foreign powers or their agents.”¹²⁴ Thus, although “prosecution [would] rarely [be] the *objective* or the result”,¹²⁵ it is clear that the House Intelligence Committee understood and endorsed the view that there could be cases, however rare, where foreign intelligence information could be sought pursuant to FISA to gather evidence to support a prosecution to protect against the activities of foreign powers and their agents.

The two Senate Reports also differentiated between government purposes. In explaining the certification requirement, the Senate Judiciary Committee Report stated that FISA was “designed to make explicit that the sole purpose of such surveillance is to secure foreign intelligence information and not to obtain information for any *other* purpose.”¹²⁶ In another portion of its Report, however, the Senate Judiciary Committee used the words “primary purpose” when it stated, “the primary purpose of electronic surveillance conducted pursuant to this chapter will not be the gathering of

¹²² 1978 House Intelligence Committee Report, *supra* note 24, at 49 (emphasis added).

¹²³ *Id.* (emphasis added).

¹²⁴ *Id.* at 62 (emphasis added).

¹²⁵ *Id.* at 24 (emphasis added).

¹²⁶ 1978 Senate Judiciary Committee Report, *supra* note 24, at 45 (emphasis added). An identical statement was made by the Senate Intelligence Committee in its report. 1978 Senate Intelligence Committee Report, *supra* note 60, at 51. *See also* 1978 Senate Judiciary Committee Report, *supra* note 24, at 39 (noting that surveillance for foreign intelligence purposes are “unlike Title III interceptions the very purpose of which is to obtain evidence of criminal activity”).

criminal evidence.”¹²⁷ In two other locations in its Report, the Senate Judiciary Committee described separate “lawful uses” of foreign intelligence information that would be permissible under the proposed legislation, which included “actual foreign intelligence purposes”, the “enforcement of criminal law”, and the deportation of an alien, “even though such use of the information is not for foreign intelligence purposes and is not for the purpose of enforcing the criminal law.”¹²⁸ The Senate Intelligence Committee also stated in its Report that the collection of intelligence information on “foreign persons” for a “noncriminal purpose” satisfied the Fourth Amendment’s “reasonable search” requirement because it applied to “surveillance conducted solely for the collection of foreign intelligence.”¹²⁹

The Senate Intelligence Committee Report also confirmed, however, that foreign intelligence collection “frequently *seeks* information needed to detect or anticipate the commission of crimes”¹³⁰ and that “U.S. persons may be authorized targets, and the surveillance is part of an investigative process often designed *to protect against* the commission of serious crimes such as espionage, sabotage, assassination, kidnapping, and terrorist acts committed by or on behalf of foreign powers.”¹³¹ The Report added:

[i]ntelligence and criminal law enforcement tend to *merge* in this area [and] surveillances conducted under [FISA] need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate.¹³²

When the House and Senate bills that led to FISA went to the Conference Committee, the conferees accepted some provisions of the House bill and some provisions of the Senate bill.¹³³ The House

¹²⁷ 1978 Senate Judiciary Committee Report, *supra* note 24, at 55.

¹²⁸ *Id.* at 53. The Senate Intelligence Committee similarly drew a distinction in its Report between “surveillance solely to collect foreign intelligence” and surveillance that is designed to “gather incriminatory evidence” because “the purpose [of the former] is unrelated to law enforcement.” 1978 Senate Intelligence Committee Report, *supra* note 60, at 14 (citation omitted).

¹²⁹ 1978 Senate Intelligence Committee Report, *supra* note 60, at 14.

¹³⁰ *Id.* at 11 n.4 (emphasis added).

¹³¹ *Id.* at 10–11 (emphasis added).

¹³² *Id.* (emphasis added).

¹³³ Reliance upon the House or the Senate Committee Reports in an effort to determine legislative intent on any particular provision of FISA requires a careful analysis of whether the House version, the Senate version, or a compromise version of the particular provision was finally approved. *Cf.*,

Conference Report contains a number of statements that further illustrate the distinction between foreign intelligence purposes and law enforcement purposes. First, the conferees agreed with the House Intelligence Committee that FISA should be codified in Title 50 and not Title 18.¹³⁴ Second, the conferees approved a provision that allowed the “use” of FISA information that was evidence of a crime for “law enforcement purposes”, which included “arrest, prosecution, and other law enforcement measures taken for the purpose of preventing the crime.”¹³⁵

A number of conclusions can be drawn from the foregoing review of FISA's legislative history.¹³⁶ First, there was, in fact, a distinction or dichotomy that existed between investigations for foreign intelligence purposes and investigations for law enforcement purposes. Second, the 1978 Congress was well aware that, notwithstanding the dichotomy, there would be instances in which the government would use the new FISA collection authority for the purpose of seeking evidence of a crime. Thus, the 1978 Congress understood that foreign intelligence purposes and law enforcement purposes were not mutually exclusive, and that FISA collection authority would be *sought* to gather criminal evidence to *protect against* international terrorism, sabotage, and clandestine intelligence activities that threatened national security. As discussed below in Part III.B, by the time the PATRIOT Act was passed, the threat to the nation had changed and with it the government's approach to protecting national security. After the 9/11 attacks, investigations would become “proactive”, and prosecutions would be part of a “preventive and disruptive” strategy.¹³⁷ Foreign intelligence and law enforcement investigations to protect national security would merge, becoming “hybrid”¹³⁸ in nature. By the time of the appeal to

1978 House Conference Committee Report, *supra* note 117, at 19 (“The conference substitute adopts the House definition.”).

¹³⁴ *Id.* at 19.

¹³⁵ *Id.* at 23.

¹³⁶ Five years after FISA was enacted, Congress conducted a review of the statute. The House stated that the government should not use FISA “once prosecution is contemplated”, unless it could “articulate reasons of national security.” H.R. REP. No. 98-738, at 6 (1984). The Senate acknowledged, however, that “it is left largely to the Executive branch to determine, in individual cases, when its purpose is to obtain foreign intelligence information and when it is to prosecute criminals.” S. REP. No. 98-660, at 14 (1984).

¹³⁷ *Reauthorization of the PATRIOT Act: Hearing Before the H. Comm. on the Judiciary*, 109th Cong. 6–7 (2005) (statement of Deputy Att’y Gen. James B. Comey).

¹³⁸ S. REP. No. 109-85, at 14 (2005) (“national security investigations are hybrid investigations with fully integrated intelligence and law enforcement components”). To

the Court of Review in 2002, the government argued for the “first time” that FISA “never adopted the bifurcation between primary purpose and criminal law purpose.”¹³⁹

B. The Significant Purpose Amendment

Two weeks after the 9/11 attacks, the Executive Branch sent Congress draft legislation¹⁴⁰ proposing that FISA’s certification requirement for both electronic surveillance and physical search applications be changed from “the purpose” to “*a purpose*” of foreign intelligence collection.¹⁴¹ In explaining the rationale of section 153, the Administration stated that the change would “eliminate the current need continually to evaluate the relative weight of criminal and intelligence purposes, and would facilitate information sharing between law enforcement and foreign intelligence authorities which is critical to the success of anti-terrorism efforts.”¹⁴²

The testimony of various Department of Justice officials made clear how important the Administration considered changing FISA’s purpose requirement. The metaphorical FISA wall had been blamed, in part, for the government’s inability to do a better job of information sharing.¹⁴³ As a

formalize the merger of intelligence and criminal investigations, the FBI “abandoned the separate case classifications for ‘criminal’ international terrorism investigations (with the classification number 265) and ‘intelligence’ international terrorism investigations (classification number 199), and [] consolidated them into a single classification for ‘international terrorism’ (new classification number 315).” *See* Letter from Steven C. McCraw, Assistant Director, Inspection Division, FBI, to Glenn Fine, Inspector Gen., U.S. Dep’t of Justice, (June 18, 2004), *available at* <http://www.usdoj.gov/oig/special/s0606/app3.htm>.

¹³⁹ Oral Argument at 51, *In re* [deleted], No. 02-001 (FISA Ct. Rev. Sept. 9, 2002), *available at* <http://www.fas.org/irp/agency/doj/fisa/hrng090902.htm>.

¹⁴⁰ *Administration’s Draft Anti-terrorism Act of 2001: Hearing Before the H. Comm. on the Judiciary*, 107th Cong. (2001), *available at* <http://judiciary.house.gov/Legacy/75288.pdf>.

¹⁴¹ Section 153 would have amended the electronic surveillance provisions of FISA, codified at 50 U.S.C. § 1804(a)(7)(B), as well as the parallel subsection of the physical search provisions, codified at 50 U.S.C. § 1823(a)(7)(B).

¹⁴² *Hearing*, *supra* note 140, at 57.

¹⁴³ *See* NAT’L COMM’N ON TERRORIST ATTACKS UPON THE U.S., FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 80 (2004), *available at* www.gpoaccess.gov/911/pdf/fullreport.pdf; OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, A REVIEW OF THE FBI’S HANDLING OF INTELLIGENCE INFORMATION PRIOR TO THE SEPTEMBER 11 ATTACKS, 30–32 (2004), *available at* <http://www.justice.gov/oig/special/s0606/final.pdf>; GOV’T ACCOUNTABILITY OFFICE, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE OF

result, and to ensure that information being collected by intelligence agents could be “communicated in a timely fashion to those criminal justice authorities who can arrest people and incapacitate them”,¹⁴⁴ the wall needed to be dismantled. For example, then-Associate Deputy Attorney General David Kris¹⁴⁵ testified at a September 24, 2001, hearing that “the animating purpose” of this portion of the draft bill was to “bring those two sides together, allow for a single unified, cohesive response, and avoid splintering and fragmentation.”¹⁴⁶

Certain members of Congress, including Senator Dianne Feinstein, remained skeptical, however, about the constitutionality of the change to “a purpose”, and her questioning of then-Attorney General Ashcroft in the Senate Judiciary Committee hearing has been credited with the birth of the significant purpose amendment.¹⁴⁷ On September 25, 2001, Senator Feinstein reiterated her concern that since “the primary purpose” test had been cited as “one of the reasons that FISA meets the constitutional requirements under the Fourth Amendment”, the elimination of the test “might place FISA in danger of being struck down by a court.”¹⁴⁸ She then asked Ashcroft what he thought about amending the Administration’s proposal to “allow for a substantial or significant purpose.”¹⁴⁹ He testified that the “overlap of criminal and terrorist activities” provided an important reason for not requiring the government to have a “single purpose” and that having to choose which purpose was “primary”, intelligence or criminal, led to the fortification of the FISA wall.¹⁵⁰ Ashcroft then stated:

if “a purpose” isn't satisfactory, saying “a significant purpose” reflects a considered judgment that would be the kind of balancing that I think we're all looking to find. If I were

COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED, GAO-01-780 (2001), *available at* www.gao.gov/cgi-bin/getrpt?GAO-01-780; BELLOWS REPORT, *supra* note 111.

¹⁴⁴ *Hearing, supra* note 140, at 35 (statement of Michael Chertoff, Assistant Att’y Gen., Criminal Division, U.S. Department of Justice).

¹⁴⁵ On March 25, 2009, David Kris was confirmed by the Senate and sworn in as the Justice Department’s Assistant Attorney General for National Security. *See* <http://www.justice.gov/nsd/bio.htm>.

¹⁴⁶ *The Intelligence to Prevent Terrorism Act of 2001 and Other Legislative Proposals in the Wake of the September 11, 2001 Attacks: Hearing Before the S. Select Committee on Intelligence*, 107th Cong., 21 (2001) (statement of David S. Kris, Associate Deputy Att’y Gen.).

¹⁴⁷ *See* Kris, *supra* note 70, at 508 n.121.

¹⁴⁸ *Homeland Defense: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 24 (2001).

¹⁴⁹ *Id.* at 25.

¹⁵⁰ *Id.*

having to choose one of your words I think that's the one I would chose.¹⁵¹

On October 3, 2001, a Senate Judiciary subcommittee held a hearing on this new proposal,¹⁵² which had been set forth in H.R. 2975, the PATRIOT Act¹⁵³ and S. 1510, the USA Act.¹⁵⁴ Although one witness called the change a “most disturbing one” because it would allow FISA collection to begin or continue even if the government had “decided that its primary purpose is to develop evidence to indict and convict somebody of a crime”,¹⁵⁵ others believed that the proposed change to FISA was constitutional.¹⁵⁶ Eight days later, the House Judiciary Committee approved H.R. 2975 and stated that the change to “a significant purpose” represented a “compromise between current law and what the Administration had proposed”¹⁵⁷ and that it would eliminate the requirement of present law for the government to “evaluate constantly the relative weight of criminal and intelligence purposes when seeking to open a FISA investigation and thereafter as it proceeds.”¹⁵⁸

Senator Patrick Leahy still remained skeptical, however, and on October 11, 2001, he stated that the proposal “raised constitutional concerns” and it would be “*up to the courts* to determine how far law enforcement agencies may use FISA for criminal investigation and

¹⁵¹ *Id.*

¹⁵² *Protecting Constitutional Freedoms in the Face of Terrorism: Hearing Before the Subcomm. on the Constitution, Federalism, and Property Rights of the S. Comm. on the Judiciary*, 107th Cong. (2001).

¹⁵³ H.R. 2975, 107th Cong. (2001).

¹⁵⁴ S. 1510, 107th Cong. (2001).

¹⁵⁵ *Hearing, supra* note 152, at 17–18 (statement of Morton H. Halperin, Chair, Advisory Board, Ctr. for Nat'l Sec. Studies, and Senior Fellow, Council on Foreign Relations, Washington, D.C.).

¹⁵⁶ *Id.* at 21–22 (statement of John O. McGinnis, Professor of Law, Benjamin N. Cardozo School of Law, Yeshiva University, New York).

¹⁵⁷ H.R. REP. No. 107-236, pt. I, at 60 (2001). Tracking legislative history often can be difficult because of amendments and substitute legislation. Nonetheless, the committee hearings that take place in regard to a predecessor bill can form an integral part of the collective legislative history of the finally enacted legislation. Although no committee reports accompanied H.R. 3162, which was the House bill that became the PATRIOT Act, H.R. 2975 was a predecessor bill to the final version of the legislation that was enacted, and hearings were conducted in regard to that bill, which contained the identical significant purpose language. As a result, H.R. REP. No. 107-236 should be considered part of the legislative history of the significant purpose amendment.

¹⁵⁸ *Id.*

prosecution.”¹⁵⁹ Senator Leahy also proposed a critical amendment that directly addressed the stated need to ensure that consultation and coordination between intelligence analysts and criminal prosecutors could take place without adversely affecting the government’s ability to use FISA. Senator Leahy’s amendment to S. 1510, which became section 504 of the PATRIOT Act, provided that intelligence and law enforcement agents may “consult” and “coordinate” their efforts, and such “[c]oordination . . . shall not preclude the certification” required by FISA or the entry of an order under FISA.¹⁶⁰

During the Senate’s debate on S. 1510, Senator Leahy stated that consultation and coordination to enforce “laws that protect against international terrorism, clandestine intelligence activities of foreign agents, and other grave foreign threats to the nation” was critical.¹⁶¹ As such, he added:

[p]rotection against these foreign-based threats by *any lawful means* is within the scope of the definition of “foreign intelligence information,” and the use of FISA *to gather evidence for the enforcement of these laws was contemplated* in the enactment of FISA.¹⁶²

Some senators were concerned as to whether the changes properly balanced the needs of law enforcement with the need to protect civil

¹⁵⁹ 147 CONG. REC. 19503 (2001) (emphasis added). By way of contrast, the 1978 Congress believed that the Legislative and Executive Branches, and not the Judicial Branch, should determine the “standards and restrictions” with respect to foreign intelligence surveillance because those decisions were intrinsically “political” in nature. *See* 1978 House Intelligence Committee Report, *supra* note 24, at 21–22 (“Under our Constitution legislation is the embodiment of just such political decisions.”).

¹⁶⁰ PATRIOT Act § 504 (codified at 50 U.S.C. §§ 1806(k), 1825(k) (2006)). *See* 50 U.S.C. § 1806(k)(1) (2006) (“Federal officers who conduct electronic surveillance to acquire foreign intelligence information” may “consult with Federal law enforcement officers” to coordinate efforts to “investigate or 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, international terrorism, or the international proliferation of weapons of mass destruction 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.”).

¹⁶¹ 147 CONG. REC. 20684 (2001).

¹⁶² *Id.* (emphasis added). A similar statement was made by Senator Leahy and other Senators in a letter sent to the FISC in July 2002. *See* Kris, *supra* note 70, at 509 n.125.

liberties.¹⁶³ Senator Feinstein, however, stated that the significant purpose amendment represented a “negotiated compromise” that was “good” because it reflected that in “today’s world things are not so simple.” In her view, the new bill’s removal of the primary purpose test would make it easier for law enforcement in “those cases where the subject of the surveillance is both a potential source of valuable intelligence and the potential target of a criminal prosecution.”¹⁶⁴

H.R. 2975 did not become law. Instead, on October 24, 2001, the House passed H.R. 3162, which combined elements of H.R. 2975, which passed the House on October 12th, and S. 1510, which passed the Senate on October 11th. In the Senate debate on H.R. 3162, Senator Leahy repeated many of the same statements that he made earlier when S. 1510 was debated, including that it would be “*up to the courts* to determine how far law enforcement agencies may use FISA for criminal investigation and prosecution beyond the scope of the statutory definition of ‘foreign intelligence information.’”¹⁶⁵ H.R. 3162 passed the Senate on October 25th and was signed by President Bush on October 26, 2001.¹⁶⁶

It is clear from the foregoing history that the 2001 Congress intended to permit prosecutors to use FISA to obtain evidence for a criminal prosecution of an agent of a foreign power, provided that a significant purpose of the FISA collection was to obtain “foreign intelligence information”, as that term is defined in FISA.¹⁶⁷ The 2001 Congress intended to break down the FISA wall, permit consultation and coordination between intelligence investigators and prosecutors, and eliminate the need for the government to determine which purpose was “primary” because in many instances the purposes would merge or overlap. It is also clear, however, that the 2001 Congress did not limit, and did not express its intent to limit, the government’s use of FISA to only certain kinds of criminal offenses.

¹⁶³ 147 CONG. REC. 19515 (2001); *see also* 147 CONG. REC. 19517 (2001).

¹⁶⁴ 147 CONG. REC. 19538 (2001).

¹⁶⁵ 147 CONG. REC. 19503 (2001) (emphasis added).

¹⁶⁶ PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

¹⁶⁷ 50 U.S.C. § 1801(e) (2006).

IV. And The Wall Came Tumbling Down

The Judiciary's first encounter with the significant purpose amendment was in the context of the government's submission of intelligence sharing procedures to the FISC that had been issued by then-Attorney General Ashcroft on March 6, 2002. Ashcroft designed the March 6th Procedures to maximize information sharing between intelligence agents and prosecutors and to take full advantage of the significant purpose amendment.¹⁶⁸ Generally speaking, the March 6th Procedures provided that prosecutors "shall have access to all information developed in full field [intelligence] investigations conducted by the FBI, including investigations in which FISA information was being used."¹⁶⁹ The March 6th Procedures specifically authorized and directed that there be consultation and coordination between intelligence agents and criminal prosecutors, and authorized prosecutors to make recommendations to the Attorney General in regard to the "initiation, operation, continuation, or expansion of FISA searches or surveillance."¹⁷⁰ The procedures also provided that consultations may include "the exchange of advice and recommendations on all issues necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities."¹⁷¹

A. *The Decision by the FISC*

After Ashcroft approved the March 6th Procedures, they were submitted to the FISC. The FISC, however, did not approve of certain portions of them, and it imposed its own requirements on the Executive Branch.¹⁷² Specifically, the FISC rejected portions of the March 6th Procedures because they authorized criminal prosecutors to provide advice to FBI intelligence officials on the "initiation, operation, continuation or

¹⁶⁸ See Kris, *supra* note 70, at 510.

¹⁶⁹ Memorandum from the Att'y Gen. to Director, FBI, Assistant Att'y Gen., Criminal Division, Counsel for Intelligence Policy and United States Attorneys, "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI" (Mar. 6, 2002) [hereinafter the March 6th Procedures], *available at* <http://www.fas.org/irp/agency/doj/fisa/ag030602.html>.

¹⁷⁰ *Id.*

¹⁷¹ *Id.*

¹⁷² See *In re All Matters Submitted to Foreign Intelligence Surveillance Court*, 218 F.Supp. 2d 611, 613 (FISA Ct. 2002).

expansion” of FISA collection.¹⁷³ While the FISC had no quarrel with improved coordination, it opposed the ability of criminal prosecutors to “direct[] FISA surveillances and searches from start to finish” and opposed the Department’s interpretation of the significant purpose amendment that allowed FISA to be “used *primarily* for a law enforcement purpose.”¹⁷⁴ Moreover, while the FISC did not object to efforts by prosecutors to “preserve” a prosecutorial “option”, it would not approve of any efforts by prosecutors to use FISA to obtain evidence for a criminal prosecution.¹⁷⁵ To ensure that prosecutors would not provide any advice that would “inadvertently” result in direction or control, the FISC imposed a “chaperone” requirement on prosecutors when they met with intelligence agents.¹⁷⁶ The FISC required that attorneys from the Office of Intelligence Policy and Review be “invited to all such consultations, and if they are unable to attend, that that office shall be apprised of the substance of the consultations forthwith in writing so that the Court may be notified at the earliest opportunity.”¹⁷⁷

B. Congressional Reaction to the FISC’s Decision

In August 2002, the Justice Department notified Congress that the FISC had “accepted in part and rejected in part the March 2002 Procedures, thus limiting the government’s ability to engage in coordination.”¹⁷⁸ Thereafter, on September 10, 2002, a hearing was held before the Senate Judiciary Committee, one day after oral argument in the government’s appeal.¹⁷⁹ At the hearing, Senator Orrin Hatch expressed his concern about the need for “effective coordination between intelligence and criminal investigations.”¹⁸⁰ In Senator Hatch’s view, the issue was “where

¹⁷³ *Id.* at 623.

¹⁷⁴ *Id.* (emphasis in original).

¹⁷⁵ *Id.*

¹⁷⁶ *Id.*

¹⁷⁷ *Id.* at 615. In March 2002, the Office of Intelligence Policy and Review was a separate component in the Justice Department. Among other responsibilities, attorneys in that office were responsible for the preparation and presentation to the FISC of all applications for electronic surveillance and physical searches pursuant to FISA. See 28 C.F.R. § 0.33a–0.33c (2005).

¹⁷⁸ See Letter from Daniel J. Bryant, Assistant Att’y Gen., to the Hon. F. James Sensenbrenner, Jr., Chairman, House Committee on the Judiciary, answer to question 21 (Aug. 26, 2002), available at <http://fas.org/irp/news/2002/10/doj101702.html>.

¹⁷⁹ See *The USA PATRIOT Act in Practice: Shedding Light on the FISA Process, Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 3 (2002) (statement of Sen. Patrick Leahy).

¹⁸⁰ *Id.* at 5 (statement of Sen. Orrin Hatch).

to draw the line between intelligence gathering and criminal investigations to ensure that our intelligence community and law enforcement agencies are fully capable of detecting and preventing future terrorist attacks while at the same time ensuring that Americans' civil liberties are preserved.”¹⁸¹ Senator Hatch praised the Justice Department for bringing the issue to the FISC and noted that the matter was pending on appeal before the Court of Review.¹⁸² Senator Arlen Specter, however, believed that the FBI and the Justice Department were “subverting the purpose of the Foreign Intelligence Act by trying to make it much, much broader than it was originally intended or that we made the modification under the PATRIOT Act.”¹⁸³

A number of witnesses testified at the September 10, 2002, Senate hearing, including then-Associate Deputy Attorney General Kris. To frame the issues, Kris provided a written statement to Congress in which he stated that at stake in the appeal for the government was:

nothing less than our ability to protect this country from foreign spies and terrorists. When we identify a spy or a terrorist, we have to pursue a coordinated, integrated, coherent response. We need all of our best people, intelligence and law enforcement alike, working together to neutralize the threat. In some cases, the best protection is prosecution In other cases, prosecution is a bad idea, and another method — such as recruitment — is called for. Sometimes you need to use both methods. But we can't make a rational decision until everyone is allowed to sit down together and brainstorm about what to do.¹⁸⁴

Thus, to the Justice Department, information sharing was “only half of the equation. The other half is advice about the conduct of the investigation going back the other way, from law enforcement to intelligence officials.”¹⁸⁵ Moreover, the government objected to the “chaperone” requirement, which impeded the ability of intelligence agents to consult with prosecutors.¹⁸⁶

¹⁸¹ *Id.*

¹⁸² *Id.*

¹⁸³ *Id.* at 8–11 (statement of Sen. Arlen Specter).

¹⁸⁴ *Id.* at 121 (statement of David Kris, Associate Deputy Att’y Gen.)

¹⁸⁵ *The USA PATRIOT Act in Practice: Shedding Light on the FISA Process, Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 122 (2002) (statement of David Kris, Associate Deputy Att’y Gen.).

¹⁸⁶ *Id.*

Kris also stated that while it was true that “[u]ltimately, the courts will decide whether or not the government’s legal arguments are persuasive”, it was equally true that those “who claim that Congress never envisioned those legal arguments [] face a steep uphill battle in light of the historical record.”¹⁸⁷

In an effort to indicate what congressional intent was when it voted on the PATRIOT ACT (and perhaps in an effort to inform the Court of Review of Congress’s intent), two weeks after the September 10, 2002, hearing, and nearly a year after the PATRIOT Act was enacted, Senator Hatch, for himself and other Senators, asked for unanimous consent for an additional statement to be included in the record of the hearing.¹⁸⁸ Senator Hatch stated that by replacing the primary purpose test with a significant purpose test:

we intended that the purpose to gather intelligence could be less than the main or dominant purpose, but nonetheless important and not *de minimis*. Because a significant purpose of gathering foreign intelligence was not the primary or dominant purpose, it was clear to us that in a FISA search or surveillance involving multiple purposes, *gathering criminal evidence could be the primary purpose* as long as gathering foreign intelligence was a significant purpose in the investigation. . . . It *was our intent* when we included the plain language of Section 218 of the U.S.A. PATRIOT Act and when we voted for the Act as a whole to change FISA to allow a foreign intelligence surveillance warrant to be obtained when “a significant” purpose of the surveillance was to gather foreign intelligence, even when the primary purpose of the surveillance was the gathering of criminal evidence.¹⁸⁹

While Senator Hatch was unambiguous in declaring that Congress had intended to permit the government to use FISA to obtain evidence in support of a criminal prosecution, his statement represents legislative future to the PATRIOT Act.¹⁹⁰ Arguably it is part of the legislative history of the

¹⁸⁷ *Id.* at 17–19.

¹⁸⁸ 148 CONG. REC. S9109 (daily ed. Sept. 24, 2002) (statement of Sen. Orrin Hatch).

¹⁸⁹ *Id.* at S9110 (emphasis added).

¹⁹⁰ *E.g.*, *United States v. Clark*, 445 U.S. 23, 33 n.9 (1980) (“[T]he view of some Congressmen as to the construction of a statute adopted years before by another Congress

Reauthorization Act as much as the 1976 and 1977 hearings are often cited as part of the legislative history of FISA.¹⁹¹ Nonetheless, even if a court were to be “remiss to ignore it”,¹⁹² Senator Hatch’s statement is silent on the issue of whether Congress intended to limit the type or nature of the crime that the government may pursue when it uses FISA. Such limitations would, however, be placed on the government by the Court of Review two months later.

C. *The Decision by the Court of Review*

The government’s 2002 appeal to the Court of Review in *In re Sealed Case* was the first appeal to that court since the enactment of FISA in 1978.¹⁹³ After receiving briefs from the government, the American Civil Liberties Union, and the National Association of Criminal Defense Lawyers and following oral argument, the Court of Review concluded that FISA, as amended by the PATRIOT Act, “supports the government’s position” and the “restrictions imposed by the FISA court are not required by FISA or the Constitution.”¹⁹⁴ The Court of Review issued a lengthy opinion in which it reviewed the legislative history of FISA, the history of the FISA wall, and the government’s assertion that a “false dichotomy” had arisen between intelligence and law enforcement investigations.¹⁹⁵ The Court of Review also reviewed the *Truong* decision and the decisions by the other federal courts and concluded that FISA “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.”¹⁹⁶

have very little, if any, significance.”) (internal quotation marks omitted); *Wright v. West*, 505 U.S. 277, 295 n.9 (1992) (expressing “grave doubts” that legislation that subsequent Congress considered but failed to enact is of “any value”).

¹⁹¹ See Seamon & Gardner, *supra* note 59.

¹⁹² See *Cannon v. Univ. of Chicago*, 441 U.S. 677, 686 n.7 (1979) (court would be “remiss” to ignore “authoritative expressions concerning the scope and purpose” of a statute).

¹⁹³ *In re Sealed Case*, 310 F.3d 717, 719 (FISA Ct. Rev. 2002).

¹⁹⁴ *Id.* at 719–20.

¹⁹⁵ *Id.* at 720–25.

¹⁹⁶ *Id.* at 725. The Court further stated that “some time in the 1980s — the exact moment is shrouded in historical mist — the Department applied the *Truong* analysis [which, as discussed above, imposed a “primary purpose” test to the electronic surveillance that had been authorized in that pre-FISA case] to an interpretation of the FISA statute.” *Id.* at 727. The Court then proceeded to discuss the July 1995 Coordination Procedures that were adopted “[a]pparently to avoid running afoul of the primary purpose test used by some courts” and pointed out how the “Department’s attitude changed somewhat” after certain

In its Supplemental Brief to the Court of Review, the government argued that the prosecution of an agent of a foreign power, even for a crime such as “mail fraud”, would serve as a “foreign intelligence purpose.”¹⁹⁷ The government contended that where it had evidence that an agent of a foreign power had engaged in espionage, prosecution for a particular offense could compromise sources and methods and “there may be no alternative but to prosecute the spy for another offense, such as mail fraud. In such a case, the mail fraud prosecution would be a ‘foreign intelligence’ purpose under FISA because it would be intended to protect against espionage.”¹⁹⁸ Thus, in the government’s view, the significant purpose amendment recognized “the Executive Branch’s expertise in identifying the information needed to protect national security from foreign threats, and the most appropriate ways of using that information.”¹⁹⁹

The Court of Review disagreed and held that the use of FISA to obtain evidence of “non-foreign intelligence” crimes “transgresses the original FISA.”²⁰⁰ Although the Court of Review did not think that the FISC should deny an application if “ordinary crimes” were “inextricably intertwined with foreign intelligence crimes”, and gave the example of a terrorist who commits bank robberies to finance terrorist activity, it stated that the “FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.”²⁰¹ However, “[s]o long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution”,²⁰² the Court of Review believed that the government would satisfy the significant purpose requirement. Accordingly, if the FISA certification “articulates a broader objective than criminal prosecution — such as stopping an ongoing conspiracy — and includes other potential non-prosecution responses, the government meets the statutory test.”²⁰³

internal reports were released. *Id.* at 728.

¹⁹⁷ Supplemental Brief for the United States at 22, *In re Sealed Case* 310 F.3d 717 (No. 02-001), available at <http://www.fas.org/irp/agency/doj/fisa/092502sup.html>.

¹⁹⁸ *Id.*

¹⁹⁹ *Id.*

²⁰⁰ *In re Sealed Case*, 310 F.3d at 735–36. While the Court of Review conceded that it “can be argued” that the PATRIOT Act “allows the government to have a primary objective of prosecuting an agent for a non-foreign intelligence crime”, that would be an “anomalous reading” of the significant purpose amendment. In its view, there was “not the slightest indication that Congress meant to give that power to the Executive Branch.” *Id.* at 736.

²⁰¹ *Id.*

²⁰² *Id.* at 735.

²⁰³ *Id.* at 736. In the Court of Review’s opinion, the certification of the purpose was to be

Thus, the Court of Review agreed with the government that by using the word “significant”, Congress eliminated “any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence purposes.”²⁰⁴

The Court of Review placed another restriction on the government, however. It stated that the government could use FISA when it intended to pursue “foreign intelligence crimes” and ordinary crimes that were “inextricably intertwined” with such crimes, but these crimes had to be “ongoing”.²⁰⁵ The Court of Review specifically ruled that FISA applications should be denied if “the government’s sole objective was merely to gain evidence of past criminal conduct — even foreign intelligence crimes — to punish the agent rather than halt ongoing espionage or terrorist activity.”²⁰⁶

After reaching its conclusions about the meaning of the statutory language, the Court of Review then turned its attention to whether the amended statute was constitutional. First, it compared Title III and FISA and considered whether the *Truong* primary purpose was the floor below which the government could not go if its actions were to be constitutional. The Court observed that when the government’s efforts are to halt espionage or terrorism “criminal prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power’s efforts.”²⁰⁷ The Court reviewed a number of Supreme Court cases decisions that approved “warrantless and even suspicionless searches” that were designed to serve the government’s “special needs, beyond the normal need for law enforcement.” Likening those needs to the foreign intelligence needs

“judged by the national security official’s articulation and not by a FISA court inquiry into the origins of an investigation nor an examination of the personnel involved.” *Id.*

²⁰⁴ *Id.* at 735.

²⁰⁵ *In re Sealed Case*, 310 F.3d 717, 735 (FISA Ct. Rev. 2002).

²⁰⁶ *Id.* Some have stated this limitation may not have any practical disadvantage to the government since it rarely has evidence gathering as its “sole objective”. See Kris, *supra* note 70. On the other hand, to the extent this prohibits the government from using FISA to collect evidence of a past foreign intelligence crime in order to charge a terrorist or spy with a crime in hope of obtaining foreign intelligence information, it does limit the government’s use of FISA.

²⁰⁷ *In re Sealed Case*, 310 F.3d at 743 (further noting that “effective counterintelligence . . . requires the wholehearted cooperation of all the government’s personnel who can be brought to the task”).

of the government, the Court of Review emphasized that “our case may well involve the most serious threat our country faces.”²⁰⁸

In the final analysis, the Court of Review found the *Keith* balancing test persuasive because it gave the legislative branch the authority to draft “different standards” in regard to foreign intelligence collection. Thus, even though the Court deemed there to be “no definitive jurisprudential answer” to whether Congress’ rejection of the primary purpose test was consistent with the Fourth Amendment, and while it did not reach the question of the President’s inherent constitutional power to conduct warrantless surveillance for foreign intelligence purposes, it concluded that the detailed statutory procedures and showings required in FISA were constitutional.²⁰⁹ As a result, even if those procedures and showings did “not meet the minimum Fourth Amendment warrant standards, [they] certainly come close.”²¹⁰ Accordingly, the Court of Review held that the amended FISA was constitutional because the surveillances and searches it authorized were “reasonable.”²¹¹ The FISC’s denial of the government’s FISA application was reversed, and the case was remanded.²¹²

The decision by the Court of Review was a major victory for the government. In the years since that decision, and, as of the time of the publication of this Article, with the exception of the *Mayfield* case,²¹³ every federal court that has ruled on the constitutionality of the significant purpose amendment has found it constitutional.²¹⁴ Although the district

²⁰⁸ *Id.* at 746.

²⁰⁹ *Id.*

²¹⁰ *Id.*

²¹¹ *Id.*

²¹² *Id.*

²¹³ *Mayfield v. United States*, 504 F. Supp. 2d 1023, 1039–40 (D. Or. 2007), *rev’d and remanded*, 599 F.3d 964 (9th Cir. 2010). After reviewing the background of FISA and the PATRIOT Act, the district court “declined to adopt the analysis and conclusion reached . . . in *In re Sealed Case*” and concluded that the amended FISA was “unconstitutional.” *Mayfield*, 504 F. Supp. 2d at 1042–43.

²¹⁴ *E.g.*, *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 307–08 (D. Conn. 2008); *United States v. Mubayyid*, 521 F. Supp. 125, 140–41 (D. Mass. 2007); *United States v. Holy Land Foundation for Relief and Development*, No. 3:04-CR-240-G, 2007 WL 2011319, at *5–6 (N.D. Tex. July 11, 2007). *Cf.* *United States v. Warsame*, 547 F. Supp. 2d 982, 996–97 (D. Minn.) (where the court expressed “very significant concerns that the ‘significant purpose’ standard violates the Fourth Amendment” but avoided deciding the issue because it concluded that “the primary purpose of the FISA surveillance and searches was to gather foreign intelligence, and was not to prosecute Warsame for criminal activity”). Other federal courts have also avoided the issue of the facial constitutionality of the statute by

court in *Mayfield* found the amended FISA unconstitutional,²¹⁵ the case was reversed on appeal for lack of standing.²¹⁶

V. Repeal of the Sunset Provision

Sixteen provisions of the PATRIOT Act, including the significant purpose amendment, were scheduled to sunset on December 31, 2005.²¹⁷ In anticipation of this deadline, between 2002 and 2005, nearly 100 hearings were held, dozens of witnesses testified, including more than 20 Justice Department officials, and the Justice Department answered more than 520 questions and more than 100 letters from members of Congress.²¹⁸ As one congressional committee put it, this was “one of the most thorough reviews of Executive branch activities under FISA” that had ever been conducted.²¹⁹ As discussed below, the hearings that took place in 2005 before the repeal of the sunset provision clearly reveal that Congress was aware of the decision by the Court of Review, the limitations it placed on the government, and possible legislative changes to address its ruling. Nonetheless, it did not explicitly accept or reject the reasoning of that court. This Part of the Article examines those 2005 hearings in detail and briefly examines hearings that took place in the 108th Congress in 2003 and 2004.

A. The 2003 and 2004 Hearings

Section 218 of FISA was briefly mentioned during three different hearings in 2003. The first hearing took place on May 20, 2003, before the House Judiciary Committee.²²⁰ Testifying for the government, then-

examining the underlying FISA applications themselves, and concluding that they meet the “primary purpose” test. *E.g.*, *United States v. Sattar*, No. 02 CR. 395 JGK, 2003 WL 22137012 at *11–12 (S.D.N.Y. September 15, 2003) (holding that the FISA collection did not violate the Fourth Amendment, “even if this Court applies the primary purpose test”), *aff’d sub nom.* *United States v. Stewart*, 590 F.3d 93, 128 (2d Cir. 2009) (“Since the interceptions meet the ‘primary purpose’ test, we, like the district court, need not and do not address Stewart’s argument that FISA’s new and less demanding ‘significant purpose’ test is unconstitutional.”); *United States v. Hammoud*, 381 F.3d 316, 333–34 (4th Cir. 2004) (“even if the primary purpose test applies, it is satisfied here”).

²¹⁵ *Mayfield*, 504 F. Supp. 2d at 1039.

²¹⁶ *Mayfield*, 599 F.3d at 973.

²¹⁷ PATRIOT Act § 224.

²¹⁸ Compare S. Rep. No. 109-85 (2005) with H.R. Rep. No. 109-174, pt. I (2005).

²¹⁹ S. Rep. No. 109-85, at 2 (2005).

²²⁰ *Anti-terrorism Investigations and the Fourth Amendment After September 11, 2001: Where and When Can Government Go to Prevent Terrorist Attacks: Hearing Before the Subcomm. on the Constitution of the*

Assistant Attorney General Viet D. Dinh testified that in the Justice Department's judgment, "the successful effort in preventing another catastrophic attack on the American homeland in the past 20 months would have been much more difficult, if not outright impossible, without the tools that Congress has authorized, in particular, the tools in the USA PATRIOT Act."²²¹ Dinh specifically mentioned that there had been a "transformation of our counterterrorism efforts, from the segregation of intelligence and law enforcement to a culture of cooperation and coordination."²²² Dinh also quoted from the decision by the Court of Review and stated that the legal rules that had developed had created what the Court of Review termed "perverse organizational incentives", expressly discouraging cooperation in the fight against terrorism.²²³ In his statement, Dinh noted the Court of Review's decision upholding the constitutionality of the new significant purpose test.²²⁴

In 2004, four hearings were held in which either section 218 or the Court of Review decision was mentioned. The first hearing took place on May 20, 2004, before the Senate Judiciary Committee.²²⁵ At that time, Senator John Cornyn specifically stated that the decision of the Court of Review "tore down the wall that stood between the intelligence officers of the United States and the criminal investigators who will be responding to the same terrorist threats" and that "[t]his increased ability to share information has disrupted terrorist operations in their early stages, . . . and has led to numerous arrests, prosecutions and convictions in terrorist cases."²²⁶

On August 23, 2004, the House Committee on Financial Services held a hearing.²²⁷ Barry Sabin, then-Chief of the Counterterrorism Section in the Criminal Division, testified that the Department believed section 218 represented a "key congressional contribution to our counterterrorism

H. Comm. on the Judiciary, 108th Cong. (2003).

²²¹ *Id.* at 6 (statement of Viet Dinh, Assistant Att'y Gen.).

²²² *Id.* at 7.

²²³ *Id.* at 9.

²²⁴ *Id.* at 10.

²²⁵ *FBI Oversight, Terrorism and Other Topics: Hearing Before the S. Comm. on the Judiciary*, 108th Cong. 1 (2004).

²²⁶ *Id.* at 7 (statement of Sen. John Cornyn).

²²⁷ *The 9/11 Commission Report: Identifying and Preventing Terrorist Financing, Hearing Before the H. Comm. on Fin. Servs.*, 108th Cong. (2004).

efforts.”²²⁸ Sabin also testified that on a “day-to-day basis”, section 218, as well as section 504, the explicit coordination provision added to the PATRIOT Act by Senator Leahy, were “essential tools that allow criminal law enforcement and intelligence folks [who] are looking at these problems to discuss and share information To allow it to sunset I believe would be setting us back to a stage where [there is] dysfunction and lack of communication and coordination.”²²⁹

John Pistole, the FBI's then-Executive Assistant Director for Counterintelligence and Counterterrorism, also testified on that same day before the House Judiciary's Subcommittee on Crime, Terrorism, and Homeland Security. He specifically referenced the decision by the Court of Review in his testimony and stated that section 218 “eliminated the wall.”²³⁰ Pistole explained the PATRIOT Act's provision for information-sharing, and the Court of Review's vindication of that legislation, had directly enhanced national security.²³¹

Section 218 was also briefly mentioned during a hearing that took place on September 13, 2004, before the Senate Judiciary's Subcommittee on Terrorism, Technology, and Homeland Security.²³² Testifying for the government, Sabin emphasized how the underlying prosecutorial culture and mission had changed, how prosecutors had become “involved earlier”, and how they now worked to “prevent” terrorist threats from being carried out.²³³ He testified that section 218 and 504 of the PATRIOT Act “enable the prosecutor . . . and the intelligence investigator to sit down, share that information, figure out which is the best tool in the tool box to use in order to address that particular threat.”²³⁴ Thus, Sabin confirmed that prosecution served a foreign intelligence purpose because prosecutors sought to prevent terrorist attacks before they occurred.²³⁵

²²⁸ *Id.* at 95 (statement of Barry Sabin, Chief, Counterterrorism Section, U.S. Dep't of Justice).

²²⁹ *Id.* at 97.

²³⁰ *Recommendations of the 9/11 Commission: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the S. Comm. on the Judiciary*, 108th Cong. 52 (2004) (statement of John Pistole, Executive Assistant Director, FBI).

²³¹ *Id.*

²³² *See Review of Tools to Fight Terrorism Act: Hearing Before the Subcomm. on Terrorism, Technology and Homeland Sec. of the S. Comm. on the Judiciary*, 108th Cong. (2004).

²³³ *Id.* at 22 (statement of Barry Sabin, Chief, Counterterrorism Section, U.S. Department of Justice).

²³⁴ *Id.*

²³⁵ *Id.*

B. The 2005 Hearings

During 2005, there were numerous hearings devoted exclusively to section 218 and the decision by the Court of Review. The first reference to the Court of Review's decision was in an April 1, 2005, letter from the Justice Department to the Senate Judiciary Committee in response to questions raised by Senator Hatch during FBI Director Robert Mueller's May 20, 2004, testimony before the Committee.²³⁶ In its letter, the Justice Department provided specific examples of cases "in which both law enforcement and intelligence interests were 'significant'", and how prosecutors and intelligence agents shared intelligence information, including FISA information, that led to indictments, criminal convictions, and sentences of numerous individuals.²³⁷ Finally, the Department also reported that it was satisfied with the decision by the Court of Review and made it clear to Congress that, from its perspective, "additional changes are unnecessary."²³⁸

The key hearings with respect to section 218 and the decision of the Court of Review took place in April and May of 2005. At an April 5th hearing before the Senate Judiciary Committee,²³⁹ Mueller testified that the PATRIOT Act had "changed the way" the FBI operates.²⁴⁰ He specifically stated that "[p]rosecutors are now involved at the earliest stages of international terrorism investigations . . . and are able to provide immediate input regarding the use of criminal charges to stop terrorist activity, including the prevention of terrorist attacks."²⁴¹ During that same hearing, Senator Feinstein specifically asked then-Attorney General Alberto Gonzales whether Congress should modify the significant purpose amendment "in any way"; Gonzales answered that it was "adequate".²⁴² In addition, while answering follow-up questions to the House Judiciary Committee, the Justice Department made a specific reference to the

²³⁶ See *FBI Oversight: Terrorism and Other Topics: Hearing Before the S. Comm. on the Judiciary*, 108th Cong. 177 (2004).

²³⁷ See *id.* at 177–78 (responses of FBI Director Robert Mueller to questions submitted by Sen. Diane Feinstein).

²³⁸ *Id.* at 181.

²³⁹ *Oversight of the USA PATRIOT Act: Hearings Before the S. Comm. on the Judiciary*, 109th Cong. (2005).

²⁴⁰ *Id.* at 9. (statement of Robert Mueller, FBI Director).

²⁴¹ *Id.* at 10.

²⁴² *Id.* at 34 (testimony of Alberto Gonzales, Att'y Gen.).

decision by the Court of Review, stating that the March 6th Procedures had been “affirmed by the Court of Review on November 18, 2002.”²⁴³ At an April 27th House Judiciary Committee hearing, other witnesses were critical of section 218 and also specifically referenced the decision by the Court of Review.²⁴⁴

On April 28th, the House Judiciary’s Subcommittee on Crime, Terrorism, and Homeland Security conducted a special hearing devoted to section 218.²⁴⁵ Patrick Fitzgerald, United States Attorney for the Northern District of Illinois, specifically referred to the Court of Review decision and provided vivid details and practical examples of the positive effects that the removal of the wall had on the government’s ability to disrupt and prevent terrorist attacks and to arrest suspected terrorists.²⁴⁶

Former Associate Deputy Attorney General David Kris also testified and prepared a detailed statement for the committee that laid out the background of the wall and the decision by the Court of Review.²⁴⁷ Kris specifically described how the Court of Review “divided crimes” into two categories — foreign intelligence crimes and ordinary crimes — and underscored the Court of Review’s holding that “FISA may be used primarily to obtain evidence of a foreign intelligence crime but not of an ordinary crime.”²⁴⁸ Kris also noted that if Congress renewed section 218, it would effectively endorse the “status quo”, by which he meant the reasoning of the Court of Review. Going further, Kris opined that the sunset should be lifted and that Congress should “explicitly” endorse the “reasoning and result of the Court of Review.”²⁴⁹

²⁴³ *USA PATRIOT Act: A Review for the Purpose of Reauthorization: Hearing Before the H. Comm. on the Judiciary*, 109th Cong. 138 (2005).

²⁴⁴ *See Implementation of the USA PATRIOT Act: Sections of the Act that Address the Foreign Intelligence Surveillance Act (FISA): Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Judiciary Comm.*, 109th Cong. 67 (2005) (statement of Gregory Nojeim, ACLU).

²⁴⁵ *See Implementation of the USA PATRIOT Act: Section 218 — Foreign Intelligence Information (“The Wall”): Hearing Before the Subcomm. On Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 109th Cong. (2005).

²⁴⁶ *See id.* at 13, 6.

²⁴⁷ *See id.* at 15–50 (statement of David Kris, Associate Deputy Att’y Gen.).

²⁴⁸ *Id.* at 27.

²⁴⁹ *Id.* at 28. Kris explained his position thus: “Whether or not you agree with its outcome, the Court of Review’s opinion is a very sophisticated and technically sound interpretation of a complex statute. If Congress were to adopt its reasoning, it would *provide guidance* that is equally sophisticated and sound. That, above all, is *what the country needs* in this area.” *Id.* (emphasis added).

Professor Peter Swire also testified at the April 28th hearing, drawing his remarks in part from a law review article that provided detailed information to the Committee about the Court of Review's decision.²⁵⁰ Among other things, Swire believed that FISA needed to be amended because the "principal purpose" of the FISA collection should be to collect foreign intelligence and not to obtain evidence of a crime.²⁵¹ While he too believed that the wall "probably deserves to be lowered somewhat in our globalized world, where information sharing is vital to fast-moving investigations", Swire also believed that the wall was "our chief bulwark against the creep of the FISA system into ordinary law enforcement."²⁵² Daniel Collins, a former Assistant United States Attorney who had served in the Department of Justice as Associate Deputy Attorney General and Chief Privacy Officer, also referenced the decision in his testimony before the Senate Judiciary Committee,²⁵³ as did Timothy Edgar, National Security Policy Counsel for the American Civil Liberties Union, in written testimony submitted to the House Intelligence Committee.²⁵⁴

Professor Richard Seamon, a former Justice Department attorney, submitted written testimony on May 11th to the House Permanent Select Committee on Intelligence.²⁵⁵ In Seamon's view, the Court of Review's interpretation of section 218 was both erroneous and overly restrictive of the government's counterterrorism efforts.²⁵⁶ According to Seamon:

[u]nder the plain language of the statute, the government should be able to seek a FISA warrant and conduct FISA surveillance for the purpose of getting the evidence needed to

²⁵⁰ See *id.* at 115 (statement of Peter Swire, Professor of Law, Ohio University). Professor Swire placed the article in the hearing record and also gave a copy to the House.

²⁵¹ *Implementation of the USA PATRIOT Act: Section 218 — Foreign Intelligence Information ("The Wall")*: Hearing Before the Subcomm. On Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary, 109th Cong. 61 (2005).

²⁵² *Id.* at 62.

²⁵³ See *Hearing on Reauthorization of the USA PATRIOT ACT: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 422 (2005) (statement of Daniel Collins, Associate Deputy Att'y Gen.).

²⁵⁴ See *Hearing on Reauthorization of the USA PATRIOT ACT: Hearing Before the H. Permanent Select Comm. on Intelligence*, 109th Cong. (2005) (statement of Timothy Edgar, National Security Policy Counsel, ACLU), available at <http://intelligence.house.gov/Media/PDFS/EdgarTestimony.pdf>.

²⁵⁵ See *id.* (statement of Richard Seamon, Associate Professor of Law, University of Idaho School of Law).

²⁵⁶ *Id.* at 2.

arrest and prosecute a foreign agent — *for any type of crime* — as long as the government reasonably considers the agent's arrest and prosecution necessary to prevent an act of international terrorism or one of the other foreign threats identified in FISA's definition of “foreign intelligence information”.²⁵⁷

Thus, in Seamon's view, the Court of Review simply got it wrong when it concluded “that the government cannot use FISA surveillance to get evidence of ‘ordinary crimes’ by a suspected terrorist”, and the arrest and prosecution of “dangerous persons” for ordinary crimes was an “important and well-established way to neutralize the danger that such persons pose.”²⁵⁸

Professor Seamon then made a specific recommendation to Congress to fix what he called the “potentially grave” misinterpretation of FISA by the Court of Review. He proposed that Congress amend the definition of foreign intelligence information to explicitly authorize the prosecutorial use of FISA when necessary to protect against the foreign threats. Seamon's intent was to “remove the restrictions on prosecutorial use of FISA surveillance that exist under *In re Sealed Case*.”²⁵⁹

On May 24, 2005, then-Associate Deputy Attorney General Kris testified before the Senate Select Committee on Intelligence.²⁶⁰ By this time, Professor Seamon's proposal had made its way into proposed legislation in the Senate.²⁶¹ Kris reiterated his “recommendation that

²⁵⁷ *Id.* at 2–3 (emphasis added).

²⁵⁸ *Id.* at 6.

²⁵⁹ Professor Seamon also made his views known to the Senate Select Committee on Intelligence in a letter, which also referenced the decision by the Court of Review. *See USA PATRIOT ACT: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 155 (2005).

²⁶⁰ *Id.* at 188 (statement of David Kris).

²⁶¹ *See* S. 1266, 109th Cong. § 202 (2005) (amending the first part of the definition of “foreign intelligence information” that relates to “protective” foreign intelligence information but leaving the second part of the definition that relates to “positive” foreign intelligence information intact). The text of the proposed language appears below in italics. Foreign intelligence information means: “(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect (*including protection by use of law enforcement methods such as criminal prosecution*) 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

Congress adopt the Court of Review’s reasoning, either through *explicit legislative history or a specific provision* of public law.”²⁶² Although Kris agreed that the proposed amendment would make it clear that “Congress’s intent” was to permit FISA to be used even if the “exclusive purpose” was to prosecute a terrorist or foreign spy, he was against the proposal and deferred to the views of the Justice Department.²⁶³ Moreover, as a policy matter, Kris did not believe that FISA should be amended unless the amendment was “genuinely necessary.” Kris supported what he called “the status quo”: renewing section 218 and codifying the Court of Review’s decision in *In re Sealed Case*. He cautioned Congress that if it renewed section 218 and enacted Seamon’s proposal, “*strong* legislative history” should be included to “guard against *any* misreading.”²⁶⁴

On June 8, 2005, then-Deputy Attorney General James Comey testified before the House Judiciary Committee. In his prepared remarks, Comey provided additional details in regard to the government’s proactive and preventative approach to national security investigations, but he sought to allay concerns that the government would use section 218 authority when its primary purpose was to investigate and prosecute crimes *unrelated* to foreign intelligence. Comey offered an example of a prosecution of an agent of a foreign power for “tax fraud”²⁶⁵ and stated that such a use of FISA had been “clearly rejected by the Court of Review”, since “the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.”²⁶⁶ In what seems to be a contradiction of this “tax fraud”

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

²⁶² *USA PATRIOT Act: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 190 (2005) (emphasis added). In a footnote to his prepared statement, Kris went further and stated “[y]our legislative staff and the Department of Justice’s Offices of Legislative Affairs and Legal Counsel would be better equipped than I am to determine the best way for Congress to express its endorsement of the Court of Review’s decision. With some Justices and judges increasingly wary of legislative history, however, an enacted provision of public law may be more authoritative than even the clearest committee report or floor statement.” *Id.* at 198. That same footnote also cited *Shannon v. United States*, 512 U.S. 573, 583 (1994), which pointed out to Congress that different members of the Supreme Court had “expressed differing views regarding the role that legislative history should play in statutory interpretation.” *Id.*

²⁶³ *Id.* at 190.

²⁶⁴ *Id.* (emphasis added).

²⁶⁵ *Reauthorization of the USA PATRIOT Act: Hearing Before the H. Comm. on the Judiciary*, 109th Cong. 14 (2005) (statement of James B. Comey, Deputy Att’y Gen.).

²⁶⁶ *Id.*

comment, however, Comey later stated that the government should “use all tools at [its] disposal to incapacitate. With Al Capone we used spitting on the sidewalk, tax charges. We do the same with counterterrorism.”²⁶⁷

The foregoing survey of legislative history demonstrates that key House and Senate Committees were keenly aware of the decision by the Court of Review and the limitations it placed on the government's ability to use FISA. Moreover, two law professors had provided specific proposals to “fix” erroneous conclusions reached by the Court of Review. Indeed, as discussed below, Professor Seamon's proposal was adopted in legislation approved by the Senate Intelligence Committee, and that Committee issued a report directly addressing one of the limitations placed on the government by the Court of Review.

C. *The Senate Bill and the House Bill*

On June 16, 2005, the Senate Intelligence Committee submitted a report on S. 1266, a bill to permanently authorize certain provisions of the PATRIOT Act.²⁶⁸ Although S. 1266 would make section 218 and nine other provisions permanent, the Senate Intelligence Committee wanted to do more than simply eliminate the sunset provision. As a result, it approved a provision to codify the change in FISA that Professor Seamon had advocated. Section 202 of the bill provided that the definition of “foreign intelligence information” in section 101(e)(1) of FISA be amended by “including protection by use of law enforcement methods such as criminal prosecution” within that definition.²⁶⁹ In its section-by-section analysis, the Senate Intelligence Committee detailed the reasoning of the Court of Review with direct citations to the court's opinion,²⁷⁰ recounting the “analytic conundrum” in which the Court of Review had found itself. In the view of the Senate Intelligence Committee,²⁷¹ the Court of Review had removed the wall, but the opinion “could also be read to put in place a

²⁶⁷ *Id.* at 48.

²⁶⁸ See S. Rep. No. 109-85 (2005).

²⁶⁹ S. 1266, 109th Cong. § 202 (2005).

²⁷⁰ See S. Rep. No. 109-85, at 9 (2005).

²⁷¹ See *id.* at 10 (“[T]he FISA process should not be used as a device to investigate ordinary crimes wholly unrelated to foreign intelligence crimes such as international terrorism, espionage, sabotage, and other hostile acts that threaten national security. However, the Court of Review recognized that sometimes even ordinary crimes might be inextricably intertwined with foreign intelligence crimes, such as when a terrorist engages in bank robberies to finance the manufacture of a bomb.”).

different kind of ‘wall’ — one that actually exists.”²⁷² The Report then quoted from the portion of the Court of Review’s decision in which it stated that if the “government’s sole objective was merely to gain evidence of past criminal conduct — even foreign intelligence crimes — to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied.”²⁷³ The Senate Intelligence Committee disagreed with this limitation on the government and agreed with the views of Professor Seamon (and others including this author) that the Court of Review went too far in its decision. The Committee viewed section 202 of S. 1266 as intending to ensure that:

FISA may be used to gain evidence to prosecute targets for their *past or future* criminal conduct involving a “foreign intelligence crime,” as that term was defined by the Court of Review in *In re: Sealed Case*. . . . Simply put, evidence of a crime related to sabotage, international terrorism, clandestine intelligence activities, or other foreign intelligence crimes (including evidence of an ordinary crime “inextricably intertwined” with a foreign intelligence crime), is a wholly included subset of the term “foreign intelligence information”.²⁷⁴

In the Committee’s view it was “perfectly permissible” to use FISA when the “intent of the collection is the protection of national security by criminal prosecution of any foreign intelligence crime the target may have committed or intends to commit.”²⁷⁵ However, the Committee deemed it impermissible to use FISA if the government’s “sole purpose was the criminal prosecution of the target for an ordinary or non-foreign intelligence crime.”²⁷⁶ In other words, “if the certifying official could certify that a significant purpose of the surveillance or physical search is to obtain foreign intelligence information about the target’s international terrorism or clandestine intelligence activities, then any incidental collection of non-foreign intelligence criminal activity would be proper”, regardless of whether the investigation focused on “past” criminal activity.²⁷⁷

²⁷² *Id.*

²⁷³ *Id.* at 11.

²⁷⁴ *Id.*

²⁷⁵ *Id.*

²⁷⁶ S. Rep. No. 109-85, at 11 (2005).

²⁷⁷ *Id.*

To ensure that a new “false dichotomy” was not erected and that no walls were “rebuilt”, the Committee approved an amendment of FISA’s definition of foreign intelligence information²⁷⁸ and stated the following in its Report:

The combined effect of Section 202’s clarification of the definition of “foreign intelligence information” with the “significant purpose” and “consultation” amendments of the USA PATRIOT Act should leave no doubt that national security investigations are hybrid investigations with fully integrated intelligence and law enforcement components. . . . The goal of Section 202 of this bill and Sections 218 and 504 of the USA PATRIOT Act is to ensure that the President is able to use all lawful means, including criminal prosecution, to prevent and neutralize threats to the national security. Simply put, Section 202 makes clear that collection of evidence via the FISA to protect national security through the prosecution of a crime related to sabotage, international terrorism, clandestine intelligence activities, or other foreign intelligence crimes (including evidence of an ordinary crime “inextricably intertwined” with a foreign intelligence crime), is an appropriate use of the FISA electronic surveillance and physical search authorities.²⁷⁹

Other Senators stated that “Congress never intended that the FISA should contain a distinction between intelligence and law enforcement activities with regard to foreign intelligence crimes Thus, rather than fundamentally changing the law governing FISA investigations, Section 202 actually restores Congress’s original intent in adopting the FISA and the ‘significant purpose’ amendment.”²⁸⁰ In endorsing Professor Seamon’s amendment, these other Senators further noted:

[w]hen a problem like this arises, Congress doesn’t have to wait for the DoJ to request legislation before it acts. As Professor Richard Seamon pointed out to the Committee in his letter on this provision, “the Department [of Justice] has

²⁷⁸ *Id.*

²⁷⁹ *Id.* at 14–15.

²⁸⁰ *Id.* at 35–36.

been wrong about this sort of thing before (having participated in building the wall).” Based on the fact that the courts are already relying on the reasoning of the Court of Review and given the DoJ role in erecting the original “wall” between intelligence and law enforcement investigators, Congress should act now to eliminate the risk that interpretations of the FISA will work to the benefit of international terrorists, spies, and others who would threaten our security.²⁸¹

While the Senate was considering its legislation, the House of Representatives was considering its own bill to permanently eliminate the sunset provisions.²⁸² Section 3 of the House bill was simple in its language and scope. With respect to the sunset provision relating to section 218 and a number of other provisions of the PATRIOT Act, it simply “repealed” the sunset provision, thereby making those provisions permanent.²⁸³ H.R. 3199 was approved by the House Judiciary Committee on July 18, 2005.²⁸⁴ The House Judiciary Committee’s Report recounted the background and need for the PATRIOT Act as well as the extensive oversight that had been conducted since 9/11.²⁸⁵ However, the Report addresses neither the reasoning of, nor the limitations placed on the government by, the Court of Review. The section-by-section analysis of the Report simply states that there was no “evidence that the Government or law enforcement was abusing the authorities of the USA PATRIOT Act.”²⁸⁶

D. Final Debate and Passage of the Reauthorization Act

On July 21, 2005, the full House began debate on H.R. 3199.²⁸⁷ The debate began on a somber note, however, because it was conducted in the shadow of the 7/7 terrorist bombings in London.²⁸⁸ Many members of

²⁸¹ *Id.* at 36.

²⁸² H.R. 3199, 109th Cong. (2005).

²⁸³ *See id.* § 3.

²⁸⁴ H.R. Rep. No. 109-174, pt. I, at 1 (2005).

²⁸⁵ *Id.* at 6–47.

²⁸⁶ *Id.* at 73–81. By way of contrast, the dissenters to the House Report were concerned that prosecutors would use FISA improperly, stating that the “long-standing policy of not letting criminal prosecutors direct intelligence investigations has been vitiated” by not allowing the significant purpose provision to sunset. *Id.* at 460.

²⁸⁷ 151 Cong. Rec. 100, H6210 (daily ed. July 21, 2005).

²⁸⁸ On July 7, 2005, bombs were detonated in three subway cars and a bus in London.

Congress did not believe that the controversial provisions of the PATRIOT Act should be made permanent. They argued that agencies had been more responsive to congressional oversight when a sunset was looming on the horizon.²⁸⁹ During the debate, however, no members of Congress addressed the issue that had been squarely placed before the legislature by the decision of the Court of Review, that had been the subject of specific hearings in Congress, and that had been the subject of testimony by current and former Justice Department prosecutors, law professors, and other expert witnesses, and that had been directly addressed by the Senate Intelligence Committee: the use of FISA for criminal prosecution. On July 21, 2005, the House passed H.R. 3199.²⁹⁰

After H.R. 3199 was passed by the House, it was sent to the Senate for debate, but the Senate substituted the text of its own bill, S. 1389, for H.R. 3199.²⁹¹ Senator Leahy stated that S. 1389 was “a good bill” and “substantially better, from a civil liberties perspective, than either the House bill, H.R. 3199, or the bill reported by the Senate Select Committee on Intelligence, S. 1266.”²⁹² When the Senate agreed to S. 1389, the amendment inspired by Professor Seamon’s proposal, section 202 of S. 1266, died. Despite having been approved by the Senate Intelligence Committee, neither S. 1266 nor the original version of H.R. 3199 were debated or voted on by the Senate. Instead, S. 1389 was passed and sent to the Conference Committee.²⁹³ The Senate debate on the Reauthorization Act took place on July 29, 2005, but it made no mention of the decision by the Court of Review.²⁹⁴ Instead, a number of Senators acknowledged that the bill was a “compromise” and “not perfect”.²⁹⁵ Thereafter, on July 29,

One week later, there was another attempted bombing of three more subway cars and a bus. *See* 7 July London Attacks, THE GUARDIAN, <http://www.guardian.co.uk/uk/july7> (last visited May 10, 2010).

²⁸⁹ *E.g.*, Extension of Remarks By Rep. Alcee Hastings, 151 Cong. Rec. E1577–1578 (daily ed. July 22, 2005); Extension of Remarks By Rep. Betty McCollum, 151 Cong. Rec. E1713 (daily ed. July 29, 2005); Remarks by Rep. Connie Mack, 151 Cong. Rec. E 1583 (daily ed. July 22, 2005); Remarks By Rep. Mark Udall, 151 Cong. Rec. E1578 (daily ed. July 22, 2005).

²⁹⁰ 151 Cong. Rec. 100, H6219 (daily ed. July 21, 2005).

²⁹¹ 151 Cong. Rec. S9558 (daily ed. July 29, 2005).

²⁹² *Id.* at S9560.

²⁹³ *See id.*

²⁹⁴ *Id.*

²⁹⁵ *Id.* (statements of Sen. Patrick Leahy and Sen. Russell Feingold).

2005, the Senate passed S. 1389,²⁹⁶ and on November 9, 2005, the House agreed to a conference with the Senate.²⁹⁷

On December 8, 2005, the Conference Committee approved the final legislation that became the Reauthorization Act. The Final Conference Report, however, did not provide any indication of whether Congress had accepted or rejected the reasoning of the Court of Review.²⁹⁸ Instead, the Report was silent on the critical questions that are the subject of this Article. The “Joint Explanatory Statement” merely states that the law makes permanent provisions of the PATRIOT Act that would have expired on December 31, 2005.²⁹⁹ On March 9, 2006, after Congress extended the expiration on two occasions,³⁰⁰ the President signed the Reauthorization Act.³⁰¹

VI. A Legislative Alternative

As discussed above, the Court of Review limited the government’s ability to use FISA in its 2002 decision of *In re Sealed Case*. First, the government may not use FISA when it intends to pursue what the Court of Review called “ordinary” or “non-foreign intelligence crimes”.³⁰² Second, even when the government intends to pursue a “foreign intelligence” crime, it may not use FISA when its “sole objective” is to gain evidence of “past criminal conduct”.³⁰³ While the second limitation seems clear, as the government cannot use FISA unless a “significant” purpose of the FISA collection is to obtain foreign intelligence information, to the extent the Court of Review’s statement limits the government’s use of FISA to the investigation of ongoing or future crimes, it represents a second limitation on the government.³⁰⁴

²⁹⁶ 151 Cong. Rec. 106, S9562–9579 (July 29, 2005).

²⁹⁷ 151 Cong. Rec. 150, H10084–10090 (Nov. 9, 2005).

²⁹⁸ H.R. Rep. No. 109-333 (2005) (Conf. Rep.), *reprinted in* 2006 U.S.C.C.A.N. 184.

²⁹⁹ *Id.* at 89.

³⁰⁰ *See* Extension of the Sunset of Certain Provisions of the USA PATRIOT Act, Pub. L. No. 109-160, 119 Stat. 2957 (2005); Extension of the Sunset of Certain Provisions of the USA PATRIOT Act, Pub. L. 109-170, 120 Stat. 3 (2006).

³⁰¹ Reauthorization Act.

³⁰² *In re Sealed Case*, 310 F. 3d 717, 731 (FISA Ct. Rev. 2002).

³⁰³ *Id.* at 735.

³⁰⁴ *Id.*

Arguably, the Court of Review asked the wrong question when it searched for, but did not find, any “indication that Congress meant to give that power” — the ability to use FISA to obtain evidence of ordinary criminal activity by an agent of a foreign power — to the Executive Branch.³⁰⁵ While the Court of Review correctly determined that section 218 eliminated the need to “balance the relative weight the government places on criminal prosecution as compared to other counterintelligence purposes”,³⁰⁶ FISA represents congressional restrictions on the Executive Branch’s ability to conduct electronic surveillance. As the Supreme Court made clear in *Keith*, Congress could establish “different standards” for the collection of “intelligence information” where “foreign powers [were] involved” that may be “compatible with the Fourth Amendment if they [were] reasonable both in relation to the legitimate need of Government for intelligence information and the protective rights of our citizens.”³⁰⁷ Thus, in the face of specific action by the 2001 Congress to alter FISA’s purpose requirement to address a legitimate need by the government to remove the FISA wall and maximize the government’s ability to collect foreign intelligence information, the Court of Review should have asked whether the legislative branch intended to limit, and whether it did limit, the government’s use of FISA to certain types of crimes.

Both “textualist”³⁰⁸ and “intentionalist” approaches to statutory interpretation should have led the Court of Review to conclude that the 2001 Congress did not limit, and did not express its intent to limit, the government’s use of FISA.³⁰⁹ Emphasizing the legislative process and

³⁰⁵ *Id.* at 736.

³⁰⁶ *Id.* at 735.

³⁰⁷ See *supra* notes 53–56 and accompanying text.

³⁰⁸ A textualist approach to statutory interpretation begins with an examination of the text of a statute. Under this approach, the plain meaning of the language governs the interpretation when the language is unambiguous. See *United States v. Ron Pair Enters.*, 489 U.S. 235, 241 (1989) (citing *Landreth Timber Co. v. Landreth*, 471 U.S. 681, 685 (1985); William N. Eskridge, Jr., *The New Textualism*, 37 UCLA L. REV. 621, 623 (1990) (“The new textualism posits that once the Court has ascertained a statute’s plain meaning, consideration of legislative history becomes irrelevant.”).

³⁰⁹ See, e.g., John F. Manning, *Textualism and Legislative Intent*, 91 VA. L. REV. 419, 423–24 (2005); Jonathan T. Molot, *The Rise and Fall of Textualism*, 106 COLUM. L. REV. 1 (2006); see also STEPHEN BREYER, *ACTIVE LIBERTY: INTERPRETING OUR DEMOCRATIC CONSTITUTION* 85–88 (2005).

Article I, section 7 of the Constitution,³¹⁰ textualists generally believe that the enacted text, rather than “unenacted legislative intent”, is always controlling.³¹¹ A textualist approach to statutory interpretation should have led the Court of Review to conclude that the government’s use of FISA was not restricted only to certain types of crimes. The text of the 2001 FISA was not ambiguous and Congress had expressed itself in plain terms. Indeed, unlike Title III, which explicitly restricts the government’s use of the criminal wiretap statute to an investigation of certain types of criminal offenses,³¹² the text of FISA does not reveal any limitations on the government’s use of FISA to only certain crimes.

The Court of Review also examined the legislative history of FISA to find congressional intent.³¹³ Under the intentionalist approach to statutory interpretation, the plainest of meaning can be trumped by contradictory legislative history if it would lead to an “absurd” result.³¹⁴ The Supreme Court has described these situations as “rare cases [in which] the literal application of a statute will produce a result demonstrably at odds with the intention of its drafters.”³¹⁵ In such circumstances, “the intention of the drafters, rather than the strict language, controls.”³¹⁶ An intentionalist approach to statutory interpretation should have led the Court of Review to conclude that the 2001 Congress had not limited the government’s use of FISA only to certain types of crimes. As illustrated above in Part III.B, when the PATRIOT Act was passed, there were no conference committee reports that accompanied the final bill.³¹⁷ Even the House Report that was approved in conjunction with a predecessor bill, H.R. 2975,³¹⁸ did not

³¹⁰ See U.S. CONST. art. I, § 7 (“Every Bill which shall have passed the House of Representatives and the Senate, shall, before it become a Law, be presented to the President of the United States.”).

³¹¹ See *INS v. Cardoza-Fonseca*, 480 U.S. 421, 453 (1987) (Scalia, J., concurring).

³¹² See 18 U.S.C. § 2516 (2006).

³¹³ *In re Sealed Case*, 310 F.3d 717, 732 (FISA Ct. Rev. 2002).

³¹⁴ See *Arlington Cent. Sch. Dist. Bd. of Educ. v. Murphy*, 548 U.S. 291, 296 (2006); Molot, *supra* note 309.

³¹⁵ *INS v. Cardoza-Fonseca*, 480 U.S. at 431 (stating that while the “ordinary and obvious meaning of the phrase is not to be lightly discounted,” the Court will look to legislative history to be certain that it did not misread the legislature’s intent.); *Tenn. Valley Auth. v. Hill*, 437 U.S. 153, 173–74 (1978) (engaging in a lengthy “examination of the language, history, and structure of the legislation” to determine what “Congress intended”).

³¹⁶ *United States v. Ron Pair Enters.*, 489 U.S. at 242; see Paul E. McGreal, *A Constitutional Defense of Legislative History*, 13 WM. & MARY BILL RTS. J. 1267 (2005).

³¹⁷ *In re Sealed Case*, 310 F.3d at 732.

³¹⁸ See H.R. Rep. No. 107-236, pt. I (2001).

indicate congressional intent to limit the government's use of FISA to certain crimes. As a review of Title III demonstrates, when Congress intends to limit the government's use of wiretap authorities, the statute contains clear limitations. When the Court of Review learned that the government might apply the statute in a manner "not anticipated by the drafters", that did not demonstrate section 218's "ambiguity"; rather, it demonstrated the section's "breadth".³¹⁹ As a result, it was arguably beyond the "province" of the Court of Review to "rescue Congress" from any drafting errors it perceived in order to reach a "preferred result".³²⁰

In its briefs before the Court of Review, the government argued for a broad reading of the statute. If the only viable method that the government has to obtain significant foreign intelligence information is to prosecute an alleged spy or terrorist for an ordinary crime, such as mail fraud or income tax evasion, then the government should be able to use FISA to obtain evidence for that prosecution.³²¹ Similarly, if the only viable way to obtain significant foreign intelligence information from an agent of a foreign power is to prosecute for what would be considered a past foreign intelligence crime, then the government should also be permitted to use FISA to obtain evidence for that prosecution. The Court of Review did state that the government's certifications are to be judged by the national security official's articulation and should "not be a FISA court inquiry into the origins of an investigation or an examination of the personnel involved",³²² thereby eliminating the need of the FISC to inquire into which purpose is primary, but the Court of Review arguably reached an erroneous statutory interpretation when it limited the government's use of FISA.

If Congress were to seek to remove the limitations placed on the government by the Court of Review, consistent with the Supreme Court's decision in *Keith*, it could enact "different standards"³²³ and approve a

³¹⁹ *Nat'l Org. for Women v. Scheidler*, 510 U.S. 249, 262 (1994) (applying the Racketeer Influenced and Corrupt Organizations Act to "situations not expressly anticipated by Congress").

³²⁰ *United States v. Granderson*, 511 U.S. 39, 68 (1994) (Kennedy, J., concurring) ("It is beyond our province to rescue Congress from its drafting errors, and to provide for what we might think . . . is the preferred result.").

³²¹ See JEFFREY BREINHOLT, *TAXING TERRORISM FROM AL CAPONE TO AL QAIDA: FIGHTING VIOLENCE THROUGH FINANCIAL REGULATION* (2005), http://www.strategycenter.net/docLib/20061007_TaxingTerrorismVoll.pdf.

³²² *In re Sealed Case*, 310 F.3d at 736.

³²³ See *supra* notes 53–56 and accompanying text.

provision comparable to the provision it has already enacted for Title III electronic surveillance. For example, Title 18, United States Code, Section 2516, provides that a federal district court judge may grant an order “authorizing or approving the interception of wire or oral communications” when the interception provides evidence of specific crimes that are enumerated in various statutes. Criminal wiretaps may only be sought, however, for offenses enumerated in the statute, which include offenses relating to “espionage”,³²⁴ “weapons of mass destruction threats”,³²⁵ “obstruction of criminal investigations”,³²⁶ and any offense involving “fraud” connected with the manufacture, importation, selling, or otherwise dealing in “dangerous drugs, punishable under any law of the United States.”³²⁷ Section 2516 also authorizes the government to file an application for a criminal wiretap in regard to “any conspiracy to commit any offense” described in section 2516.³²⁸

Following this approach, a new subsection of FISA, which could be codified at 50 U.S.C. § 1804(f) (and in the corresponding subsections in the other applicable provisions of FISA), should be added to make clear that if the government is seeking to obtain *protective* foreign intelligence information — that is, foreign intelligence information that can protect the United States against the hostile actions of foreign powers and their agents as described in section 1801(e)(1)³²⁹ — then the government may use FISA regardless of the type or nature of the crime it intends to pursue. One possible suggested wording of that subsection would be as follows:

(f) Investigation of Criminal Offenses — An application for an order approving electronic surveillance to seek foreign intelligence information within the meaning of section 106(e)(1) of FISA may be sought by a Federal officer regardless of the nature and type criminal offense, if any, which may be pursued by the government, provided that a significant purpose of the application is to obtain foreign intelligence information and each of the other requirements

³²⁴ 18 U.S.C. § 2516(1)(a) (2006).

³²⁵ *Id.* § 2516(1)(c).

³²⁶ *Id.*

³²⁷ *Id.* § 2516(1)(e).

³²⁸ *Id.* § 2516(1)(s).

³²⁹ *See supra* notes 71–72 and accompanying text.

of the statute have been established in accordance with this subchapter.

Finally, to make explicit its intent to remove the limitations placed on the government by the Court of Review, at the time of passage of this amendment to FISA, both houses of Congress should approve a Final Conference Report that makes specific reference to that decision and explicitly states congressional intent to remove the limitations placed on the government in accordance with this proposed change.

This proposed amendment would not change who may be targeted under FISA; that is, only targets who meet FISA's definition of foreign powers and agents of foreign powers would qualify as FISA targets. This proposed amendment also would not change the factual showing that the government would be required to make to the FISC; that is, the government would still be required to establish probable cause and meet other requirements of the statute. As they pertain to investigations of U.S. persons, these requirements largely center on the criminal activity of the target of the FISA collection. This proposed amendment would, however, enable the government to use FISA to protect national security, regardless of the nature and type of crime that the Executive Branch concludes is the best prosecutorial vehicle to obtain significant foreign intelligence information.

VII. Conclusion

Important lessons emerge from an examination of the legislative history of FISA's significant purpose amendment, the decision by the Court of Review, and congressional reaction to that decision. First, while this author agrees with the position taken by the government before the Court of Review and does not agree with the limitations placed on it by that Court, even assuming *arguendo* that those limitations are appropriate, they were not placed on the government by the legislative branch in an explicit manner prior to the original passage of the significant purpose amendment. Congress was keenly aware of the limitations placed on the government by the Court of Review as well as a legislative alternative that would have removed those limitations, but Congress rejected that alternative. As a result, while the lack of an explicit congressional expression of its intent does not affect the manner in which the Judiciary should interpret FISA now that

the sunset provision has been permanently eliminated,³³⁰ the better legislative approach would have been for Congress to have explicitly expressed its will in a final conference report prior to the passage of the Reauthorization Act.

The government should be permitted to use FISA to obtain significant foreign intelligence information to disrupt a terrorist plot or foil a spy network even if it intends to prosecute a past foreign intelligence crime or an ordinary crime. Legitimate debate will continue between those who believe that if we “give up essential liberty to obtain a little temporary safety [we] deserve neither liberty nor safety”³³¹ and those who believe that “[t]he Constitution is not a ‘suicide pact’.”³³² But we do not need to choose between the two because liberty and security are not mutually exclusive. At this time in our Nation’s history, the Constitution will not “break”³³³ if the limitations placed on the government by the Court of Review are removed. Provided that each of its requirements has been satisfied, including that a significant purpose of the FISA collection is to obtain foreign intelligence information, the government should be able to use FISA to protect against the threats posed by alleged terrorists and spies, regardless of the type or nature of the crime that the government chooses to pursue.³³⁴

³³⁰ See *Cannon v. Univ. of Chicago*, 441 U.S. 677, 696–699 (1979) (when Congress enacts statutory language identical to other provisions, it is not only appropriate but also realistic to presume that “Congress was thoroughly familiar with . . . important precedents” construing that language and “expected its enactment to be interpreted in conformity with [them]”); *Lorillard v. Pons*, 434 U.S. 575, 580 (1978) (“Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it reenacts the statute without change.”).

³³¹ See BENJAMIN FRANKLIN, *HISTORICAL REVIEW OF PENNSYLVANIA* (1759), as reproduced in JOHN BARTLETT, *FAMILIAR QUOTATIONS* 422 (Emily Morrison Beck ed., Little Brown and Company, 14th ed. 1968).

³³² See *Terminiello v. Chicago*, 337 U.S. 1, 37 (1949) (Jackson, J., dissenting).

³³³ See RICHARD A. POSNER, *NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY* 1 (2006) (“marginal adjustments” in constitutional rights should be made by “practical-minded judges” when the “values that underline the rights — values such as personal liberty and privacy — come into conflict with values of equal importance, such as public safety, suddenly magnified by the onset of a national emergency” so that the Constitution will not “break”).

³³⁴ See *In re Sealed Case*, 310 F.3d 717, 724 (FISA Ct. Rev. 2002) (“arresting and prosecuting [foreign agents] may well be the best technique to prevent them from successfully continuing their terrorist or espionage activity”); Seamon & Gardner, *supra* note 59, at 325 (the restrictions placed on the government by the Court of Review prevent it from taking spies and terrorists “off the street”).