THE PATRIOT ACT AND THE WALL BETWEEN FOREIGN INTELLIGENCE AND LAW ENFORCEMENT

RICHARD HENRY SEAMON* AND WILLIAM DYLAN GARDNER**

* Associate Professor of Law, University of Idaho. This article discusses events in the U.S. Department of Justice from the 1980s to the present. For part of that period (1990-1996), I worked in the Department as an Assistant to the Solicitor General of the United States. I do not remember working directly on any of the matters discussed in this article. In any event, the opinions expressed in this article are solely mine and my coauthor's. We thank the following people for reviewing or commenting on all or parts of drafts of this article: Stewart A. Baker, William C. Banks, Stephen Dycus, William F. Funk, Max Kidalov, David Kris, Philip A. Lacovara, Robert Pikowsky, Peter Raven-Hansen, and Kim Lane Scheppele.

** J.D., 2004, University of South Carolina School of Law.

Ever since its hurried enactment six weeks after the 9/11 terrorist attacks, the USA PATRIOT Act[1] has generated confusion and controversy. One thing about the Act upon which most people agree, however, is that it expanded government power to combat terrorism.[2] In particular, the Act supposedly tore down "the wall" between

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

[2] *See, e.g.*, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 394 (2004) [hereinafter 9/11 COMM'N REPORT) ("[T]he Patriot Act . . . vested substantial new powers in the investigative agencies of the government.").

foreign intelligence and criminal law enforcement.[3] According to a recent federal court decision, however, the Patriot Act did not raze the wall; to the contrary, the Act raised, for the first time, a statutory basis for the wall.[4] On that view, the Patriot Act restricts, rather than expands, the government's power to fight terrorism.[5] This article argues that the court interpreted the Patriot Act incorrectly; but so did the federal courts that interpreted prior legislation to create the wall in the first place. The article urges Congress to clarify the matter—and truly tear down the wall—when it reauthorizes the Patriot Act.

This article focuses on "one of the most important"[6] and "perhaps the most controversial"[7] provision in the Patriot Act. That provision amended the Foreign Intelligence Surveillance Act of 1978 (the FISA).[8] The FISA was enacted to regulate the executive branch's use of electronic surveillance to get foreign intelligence information.[9] The

---

[3] *See e.g., id.* at 328 (stating that "[a] central provision" of the Administration proposal that became the Patriot Act "was the removal of 'the wall' on information sharing between the intelligence and law enforcement communities . . . ."); U.S. Department of Justice, Office of the Inspector General, Audit Division, *The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information*, Audit Report 04-10, at 2 (Dec. 2003) ("The Patriot Act lifted legal barriers to the sharing of foreign intelligence information between the federal intelligence community and the federal law enforcement community."); Robert S. Mueller III, Prepared Statement Before the 9/11 Commission 2 (Apr. 14, 2004) (transcript available at http://www.fbi.gov/congress/congress04/mueller041404.htm) ("The PATRIOT Act, the Attorney General's intelligence sharing procedures and the opinion from the Foreign Intelligence Surveillance Court of Review tore down the legal impediments to coordination and information-sharing between criminal investigators and intelligence agents."); Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663, 688 (2004) (provisions in Patriot Act "tear down th[e] wall"); Kim Lane Scheppele, *Law in a Time of Emergency: States of Exception and the Temptations of 9/11*, 6 U. PA. J. CONST. L. 1001, 1038 (2004) (stating that, after Patriot Act's enactment, "it was only a matter of time before the wall collapsed"); Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1327 (2004) (describing "the breaking down of the 'wall' between foreign intelligence and law enforcement activities" as "perhaps the most controversial change in FISA in the Patriot Act"). *See generally* THE 9/11 COMM'N REPORT, *supra* note 2, at 78–80 (summarizing development of "the wall"); Eleanor Hill, Staff Director, *Joint Inquiry Staff Statement for Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001* 21–26 (Oct. 8, 2002) [hereinafter *Joint Inquiry Staff Statement*], *available at* http://intelligence.senate.gov/0210hrg/021008/hill.pdf.

[4] *See In re* Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002); *see also infra* notes 346–413 (discussing this case).

[5] *See infra* notes 418–19 & 649–52 and accompanying text.

[6] Erwin Chemerinsky, *Losing Liberties: Applying a Foreign Intelligence Model to Domestic Law Enforcement*, 51 UCLA L. REV. 1619, 1626 (2004).

[7] Swire, *supra* note 3, at 1327.

[8] Patriot Act, § 218, 115 Stat. 291 (amending 50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B)). The FISA is codified at 50 U.S.C. §§ 1801–1862.

[9] *See infra* notes 58–71 and accompanying text (discussing forces leading to FISA's enactment).

FISA generally requires the government to have advance judicial approval for such surveillance. To get judicial approval for electronic surveillance under the original FISA, a high-ranking government official with intelligence responsibilities had to certify to a court that "the purpose of the surveillance was to obtain foreign intelligence information."[10] Some lower federal courts interpreted this provision to mean that the "primary purpose" of the proposed surveillance had to be gathering foreign intelligence, rather than gathering evidence for a criminal prosecution.[11] This "primary purpose" test assumed incompatibility between the purpose of gathering foreign intelligence and the purpose of gathering evidence for a prosecution. To satisfy the primary purpose test, the Department of Justice accordingly adopted procedures limiting contact between foreign intelligence agents in the FBI and federal prosecutors. Those procedures came to be interpreted restrictively by the Justice Department and the court responsible for issuing FISA surveillance orders, the Foreign Intelligence Surveillance Court ("FISA Trial Court"). The restrictive interpretation produced what the public came to call "the wall."[12] The wall thus was mainly the result of (1) lower courts' interpretation of the original FISA's "purpose" provision; (2) the Justice Department's procedures for implementing the lower courts' interpretation; and (3) the restrictive interpretation of those procedures by Department officials and the FISA Trial Court.[13]

The wall caused trouble before 9/11 but did not attract public or congressional attention until afterwards.[14] For example, the wall hurt

---

[10] 50 U.S.C. § 1804(a)(7)(B) (1980).

[11] *See infra* notes 210–23 and accompanying text.

[12] *See infra* notes 227–86 and accompanying text.

[13] "The wall" originally referred to restrictions on intelligence sharing internal to the U.S. Department of Justice. *See, e.g., 9/11 Comm'n Staff Statement No. 9*, at 4–5 (*available at* http://www.9-11commission.gov/staff_statements/ staff_statement_9.pdf) (stating that internal Justice Department procedures to separate foreign intelligence functions from law enforcement functions "became known as the 'wall'"); *see also infra* notes 227–86 and accompanying text. The phrase came to be used in a broader sense to mean "a series of restrictions" between foreign intelligence and law enforcement that existed "between and within" various federal agencies and that was "constructed over sixty years as a result of legal, policy, institutional, and personal factors." HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE AND THE SENATE SELECT COMMITTEE ON INTELLIGENCE, REPORT OF THE JOINT INQUIRY INTO THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, S. REP. NO. 107-351 & H.R. REP. NO. 107-792, at 363 (Dec. 2002) (pagination from unclassified version of report) [hereinafter REPORT OF THE JOINT INQUIRY]; *see also* Hill, *Joint Inquiry Staff Statement*, *supra* note 3, at 21–26 (referring to "the many 'walls' that have been built between the agencies over the past sixty years").

[14] *See, e.g.*, Hill, *Joint Inquiry Staff Statement*, *supra* note 3, at 14 ("The walls that had developed to separate intelligence and law enforcement often hindered efforts to

the investigation of whether Wen Ho Lee stole classified information from the Los Alamos National Laboratory.[15] It was the 9/11 attacks, however, that made the general public aware of the wall, because of its apparent role in the government's failure to prevent the 9/11 attacks.[16] Right after 9/11, the Justice Department asked Congress to amend the "purpose" provision of the original FISA to eliminate the primary purpose test. Under the Department's proposal, instead of certifying that "*the* purpose" of proposed FISA surveillance was to obtain foreign intelligence information, the government would have to certify that obtaining foreign intelligence was "*a* purpose" of the proposed surveillance.[17] Rather than adopt that proposal, Congress amended the original FISA in the Patriot Act to require the government to show that obtaining foreign intelligence information is "*a significant* purpose" of the proposed surveillance.[18] Congress thus struck a compromise between the Department of Justice and supporters of the primary purpose test.

The case on which this article focuses arose when the Justice Department changed its procedures to implement the Patriot Act's "significant purpose" amendment. The new procedures reflected the Department's view that the Patriot Act eliminated the primary purpose test. Thus, the Department's procedures allowed the government to seek judicial orders approving electronic surveillance under the FISA for the primary purpose of building a prosecution. The Department sought approval of the new procedures by the FISA Trial Court. The FISA Trial Court largely rejected them, however, concluding that the Patriot Act did not eliminate the "primary purpose" test.[19] The Department took its first-ever appeal to the Foreign Intelligence Surveillance Court of Review ("FISA Court of Review" or "Court of Review"). In its first-ever decision, called In re *Sealed Case*, the FISA Court of Review reversed the FISA Trial Court.[20] To begin with, the Court of Review held that the primary purpose test misread the original FISA of 1978; the test was based on

---

investigate terrorist operations aggressively.").

[15] *See infra* notes 264–65 and accompanying text.

[16] *See infra* notes 266–86 and accompanying text.

[17] *See infra* notes 287–91 and accompanying text.

[18] 50 U.S.C. § 1804(a)(7)(b) (2002) (emphasis added). The Patriot Act also added a provision to the FISA expressly authorizing coordination of law enforcement activities and intelligence activities in investigations involving FISA surveillance. *See* 50 U.S.C. § 1806(k), discussed *infra* notes 302–03 and accompanying text.

[19] *See In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 614–25 (2002) [hereinafter FISA Trial Court Opinion].

[20] *In re* Sealed Case, 310 F.3d 717, 746 (Foreign Int. Surv. Ct. Rev. 2002).

a "false dichotomy" between foreign intelligence and law enforcement.[21] In a curious twist, however, the Court of Review found that the Patriot Act amended the FISA to ratify that "false dichotomy." "In short," the FISA Court of Review said, "even though . . . the original FISA did not contemplate the 'false dichotomy' [between foreign intelligence and law enforcement] the Patriot Act actually did—which makes it no longer false."[22] Faced with this "analytic conundrum,"[23] the FISA Court of Review interpreted the FISA, as amended by the Patriot Act, to relax the restrictions associated with the primary purpose test but not to eliminate them altogether.

Specifically, the Court of Review interpreted the FISA, as amended by the Patriot Act, to restrict the government's use of FISA surveillance for law enforcement purposes in two ways. First, the government cannot use FISA surveillance if its sole objective is to prosecute foreign agents for past crimes, even for foreign intelligence crimes such as espionage and international terrorism.[24] Under this restriction, for example, after the 9/11 attacks the government could not have gotten a FISA order solely to gather evidence of Jose Padilla's past involvement in those attacks.[25] The government would need a future-oriented objective as well, such as the prevention of future acts of terrorism. Second, the government cannot use FISA surveillance if its primary (much less its sole) objective is to prosecute foreign agents for "non-foreign intelligence crimes."[26] Thus, for example, the government could not use FISA surveillance for the primary purpose of prosecuting a suspected terrorist of cocaine dealing if the cocaine dealing served only to support the suspect's own drug habit and not to fund her terrorist activity. This restriction prevents the government from using FISA surveillance to take foreign agents "off the street" by getting evidence to arrest and prosecute them for ordinary crimes. The Court of Review admitted that its

---

[21] *Id.* at 735.

[22] *Id.*

[23] *Id.*

[24] *Id.*. The court limited this holding to foreign agents who are "United States persons," a term that includes U.S. citizens and permanent resident aliens. *See* 50 U.S.C. § 1801(i) (2002) (defining "United States person" for purposes of FISA).

[25] *See, e.g.*, Richard B. Schmitt, *Government Says Padilla Plotted High-Rise Attacks; Allegations Are Released as the Supreme Court Prepares to Rule on His Arrest and Detention*, L.A. TIMES, June 2, 2004, at A1 (reporting government's allegation that, "in addition to wanting to plant a 'dirty bomb,' [Padilla] also plotted with Al Qaeda to blow up high-rise apartment buildings in the United States").

[26] *In re* Sealed Case, 310 F.3d at 736.

restrictive reading of the FISA was "paradoxical,"[27] because the Patriot Act was meant to expand executive power, whereas the original FISA was meant to restrict it.

The Court of Review made clear, however, that the Patriot Act erects a lower wall than the one associated with the primary purpose test. The Court of Review thus rejected the FISA Trial Court's conclusion that, even as amended by the Patriot Act, the FISA continues to impose the primary purpose test.[28] The Court of Review also rejected the argument of amici curiae on appeal that the Fourth Amendment requires the government to meet the primary purpose test to obtain a FISA surveillance order.[29] Instead, the Court of Review held as a matter of statutory interpretation and Fourth Amendment law that the government can get a FISA surveillance order if its primary purpose is to investigate and prosecute "foreign intelligence crimes," as long as it also has a significant foreign intelligence purpose other than prosecutorial use. (As mentioned above, however, the court construed the FISA to prohibit the government from getting a FISA order if its sole objective is to investigate and prosecute foreign intelligence crimes; or if its primary (or sole) purpose is to prosecute a "non-foreign intelligence crime.") Given the Court of Review's rejection of the primary purpose test, the federal government considered the court's decision a victory and did not seek U.S. Supreme Court review.

While the FISA Court of Review's Fourth Amendment ruling has generated much commentary,[30] its statutory rulings have attracted

---

[27] *Id.* at 734.

[28] *Id.* at 732–34.

[29] *Id.* at 736–46.

[30] *See* William C. Banks, *And The Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1150 (2003) (arguing that decisions of FISA Trial Court and FISA Court of Review contained both statutory and constitutional errors); Rebecca A. Copeland, *War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America*, 35 TEX. TECH L. REV. 1, 3 (2004) (focusing on effects of post-9/11 legal changes on constitutional freedoms); Michael P. O'Connor & Celia Rumann, *Going, Going, Gone: Sealing the Fate of the Fourth Amendment*, 26 FORDHAM INT'L L.J. 1234, 1238 (2003) (focusing on how FISA Court of Review's decision violates the Fourth Amendment); Scheppele, *supra* note 3, at 1043–47 (implying that, as implemented by Attorney General, Patriot Act's amendments to FISA's "purpose" provision violate the Fourth Amendment); Ronald J. Sievert, *War on Terrorism or Global Law Enforcement Operation?*, 78 NOTRE DAME L. REV. 307, 336–37 & nn.158–59 (2003) (stating that "constitutional underpinnings" of FISA depend on its being interpreted, even as amended by Patriot Act, "as an intelligence tool"); John C. Yoo, *Judicial Review and the War on Terrorism*, 72 GEO. WASH. L. REV. 427, 442–44 (2003) (discussing case law and statutory provisions on "primary purpose" test in context of exploring constitutional boundaries of judicial review of war powers); Nola K. Breglio, Note, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence*

little.[31] This article seeks to fill the gap by addressing the statutory rulings, and, in the process, takes a position contrary to that taken in the scant commentary on those rulings that does exist.[32] The court's statutory rulings deserve attention for three reasons. First, issues of statutory interpretation affect the existence and nature of the Fourth Amendment issues posed by FISA surveillance. Most fundamentally, the question whether FISA surveillance satisfies the Fourth Amendment depends on what the FISA means. Second, the court's statutory rulings restrict the government's ability to fight international terrorism right now. The restrictions are less severe than those associated with the primary purpose test, and they may be wise policy, but they could still have grave results.

Surveillance, 113 YALE L.J. 179, 180 (2003) (arguing that Patriot Act, as interpreted by FISA Court of Review, causes FISA procedures "no longer" to "provide constitutionally adequate protection"); David Hardin, Note, *The Fuss Over Two Small Words: The Unconstitutionality of the USA PATRIOT Act's Amendments to FISA Under the Fourth Amendment*, 71 GEO. WASH L. REV. 291 (2003) (discussing constitutional analysis); Heath H. Galloway, Note, *Don't Forget What We're Fighting For: Will the Fourth Amendment Be a Casualty of the War on Terror?*, 59 WASH & LEE L. REV. 921 (2003) (discussing Patriot Act's effect on civil liberties); Grayson A. Hoffman, Note, *Litigating Terrorism: The New FISA Regime, the Wall, and the Fourth Amendment*, 40 AM. CRIM. L. REV. 1655, 1659 (2003) (arguing that FISA Court of Review's Fourth Amendment analysis is substantially correct); Stephanie Kornblum, Note, *Winning the Battle While Losing the War: Ramifications of the Foreign Intelligence Surveillance Court of Review's First Decision*, 27 SEATTLE U. L. REV. 623, 648–56 (2003) (arguing that FISA Court of Review's unnecessarily broad decision exposes FISA, as amended by Patriot Act to constitutional challenges); George P. Varghese, Comment, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385, 386 (2003) ("call[ing] into question the constitutionality of the Patriot Act's 'significant purpose' test").

[31] Banks, *supra* note 30, at 1167–81 (arguing that FISA Trial Court was correct to prohibit Criminal Division control of FISA surveillance and that FISA Court of Review's reversal of FISA Trial Court rested on misunderstanding of FISA); John E. Branch III, Recent Development, *Statutory Misinterpretation: The Foreign Intelligence Court of Review's Interpretation of the 'Significant Purpose' Requirement of the Foreign Intelligence Surveillance Act*, 81 N.C. L. REV. 2075, 2076 (2003) (arguing that FISA Court of Review's opinion "goes too far in eroding restrictions on the government's use of FISA searches to the extent that it invites abuse of those searches"); *cf.* Daniel Richman, *Prosecutors and Their Agents, Agents and Their Prosecutors*, 103 COLUM. L. REV. 749, 822–24 (2003) (explaining that "there may be countervailing benefits from relaxation of strictures," such as the Patriot Act's relaxation of the "primary purpose" test); Rosenzweig, *supra* note 3, at 686–91 (discussing the wall and defending Patriot Act's modification of it primarily on policy grounds).

[32] *See* Banks, *supra* note 30, at 1174–81 (statutory analysis concluding that overall FISA Trial Court's opinion was faithful to "the very core objective of FISA, even as amended by the Patriot Act" and that FISA Court of Review reversed trial court based on misreading of statute); Branch, *supra* note 31, at 2078–79 (summarizing argument that the FISA Court of Review's interpretation makes it too easy for government to use FISA surveillance for prosecutorial purposes); Swire, *supra* note 3, at 49–51 (brief statutory analysis concluding that FISA Trial Court correctly interpreted original FISA but not FISA as amended by Patriot Act; and that FISA Court of Review interpreted FISA, as amended by Patriot Act, to make it too easy for government to use FISA surveillance for prosecutorial purposes).

Third, the statutory rulings will need Congress's attention when it debates reauthorization of the Patriot Act. The provision in the Patriot Act amending the "purpose" provision of the original FISA sunsets in December 2005.[33] Congress has the options of (1) allowing the sunset to occur, in which case the original version of FISA's purpose provision comes back into force; (2) reauthorizing the current Patriot Act provision that amends the original FISA's purpose provision; or (3) clarifying or substantively changing the statutory law on the permissible purposes of FISA surveillance. If Congress chooses the first option and the original FISA comes back into force, its meaning will immediately be the subject of a conflict between the FISA Court of Review and the circuits that construed the original FISA to impose the "primary purpose" test. If Congress elects the second option and simply reauthorizes the Patriot Act provisions that alter the primary purpose test, a conflict among the federal courts about the meaning and constitutionality of those provisions is likely to develop. If Congress takes the third option by considering statutory changes, it must address the important issue of the proper degree of separation between law enforcement agents and intelligence agents.[34] A proper choice among these options depends on a "full and informed debate."[35] This article seeks to inform the debate, as well as to guide courts in pending and future prosecutions in which the government seeks to use evidence obtained through surveillance under the current version of the FISA.

The article addresses the statutory foundation for "the wall" in four steps. Part I describes the origin of the primary purpose test and the wall associated with that test. In addition to providing necessary background, Part I lays the groundwork for statutory analysis by closely examining the text of the relevant statutory provisions. Part II describes the events leading to In re *Sealed Case* and the decisions in the case. Part II's description of the FISA Court of Review's decision

---

[33] Patriot Act, § 224(a), 115 Stat. 295 (2001) (providing that, with certain exceptions, provisions including § 218 of Patriot Act, which amended 50 U.S.C. § 1804(a)(7)(B) to replace "the purpose" with "a significant purpose," expire on December 31, 2005), reproduced as note after 50 U.S.C. § 1802.

[34] This issue extends beyond the proper scope of the government's authority to get approval for electronic surveillance under the FISA. The divide between law enforcement and foreign intelligence has deep roots. One major example of the division is reflected in, and effected by, the statute that bars the CIA from exercising domestic law enforcement powers. *See* National Security Act of 1947, ch. 343, § 102(d)(3), Pub. L. No. 80-253, 61 Stat. 495 (1947), codified at 50 U.S.C. § 403-3(d)(1) ("[T]he Agency shall have no police, subpoena, or law enforcement powers or internal security functions.").

[35] 9/11 COMM'N REPORT, *supra* note 2, at 394.

identifies some of the relevant legislative history. This aspect of Part II, like Part I's examination of statutory text, lays groundwork for the statutory analysis in Part III. Part III explains the importance of the statutory issues and then analyzes them, building on Parts I and II. Part III concludes that the FISA Court of Review misread both the original FISA and the Patriot Act. The FISA Court of Review correctly concluded that the original FISA did not compel the primary purpose test. The Court of Review failed to recognize, however, that the original FISA did limit the government's use of foreign intelligence information for law enforcement purposes. Properly read, the original FISA prohibited the government from using FISA surveillance to get information for a prosecution, unless the government intended the prosecution to serve one or more of the five foreign intelligence purposes prescribed in the FISA. In short, the original FISA restricted government surveillance more than the FISA Court of Review believed, but less than those courts adopting the primary purpose test believed.

As amended by the Patriot Act, the FISA does not impose either the primary purpose test or the lesser restrictions discerned by the Court of Review. Like the original FISA, the FISA as amended by the Patriot Act allows the government to conduct FISA surveillance for the primary – or even the sole – purpose of getting evidence for a prosecution. Moreover, the anticipated prosecution can involve any type of crime, not just "foreign intelligence crimes." This prosecutorial objective for conducting FISA surveillance remains subject to an important restriction. The government must intend the anticipated prosecution to serve one or more of the five foreign intelligence purposes identified in the FISA.

In sum, Parts I through III stake out the position that all of the significant case law is wrong. The FISA Court of Review, as well as the FISA Trial Court, misinterpreted both the original FISA and the Patriot Act; pre-Patriot Act case law establishing the "primary purpose" test is also wrong. Recognizing that the statutory issues are debatable and highly unsettled, however, Part IV of the article proposes an amendment to the FISA that (assuming one accepts the article's statutory interpretation) clarifies its meaning.

I. LEGENDS OF THE WALL

According to legend, the Roman Emperor Caligula "wrote his laws

in a very small character, and hung them up upon high pillars, the more effectually to ensnare the people."[36] The Foreign Intelligence Surveillance Act (FISA) is caligulan in its inaccessibility, which prompts the detailed attempt in this Part to separate legend from reality. After a brief historical discussion in Section A, Section B examines the FISA's text closely. That examination lays groundwork for understanding the cases and the Department of Justice actions, described respectively in Sections C and D, that built "the wall" on top of the original FISA. Section E describes the Patriot Act's supposed demolition of the wall.

A. Pre-FISA

Before Congress enacted the Foreign Intelligence Surveillance Act ("FISA") in 1978, presidents beginning with Franklin Roosevelt authorized warrantless electronic surveillance in the name of national security. They claimed the "inherent power" to do so.[37] The power supposedly inhered in the "President's constitutional duty to act for the United States in the field of foreign affairs . . . [and] to protect national security."[38]

In 1968, Congress enacted legislation regulating the executive branch's use of electronic surveillance to investigate crime, but not its use for national security purposes.[39] The 1968 legislation, Title III of the Omnibus Crime Control and Safe Streets Act ("Title III"), generally required the government to get advance judicial approval for electronic surveillance to investigate crime.[40] Title III also, however, contained a two-sentence proviso disclaiming an intention to address the President's power to use electronic surveillance for national security. The proviso's first sentence covered the President's power to deal with foreign threats to national security:

> Nothing contained in this chapter . . . shall limit the constitutional power of the President [1] to take such measures as he deems necessary to protect the Nation against actual or potential attack or

---

[36] 1 WILLIAM BLACKSTONE, COMMENTARIES *46.

[37] United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 310–11 n.10 (1972); S. REP. NO. 95-604, at 7 (1978) ("[E]very President since Franklin D. Roosevelt asserted the authority to authorize warrantless electronic surveillance and exercised that authority."); *id.* at 10–12 (detailing this history); *see also* H.R. REP. NO. 95-1283, Pt. I, at 15–16 (1978) (discussing history of warrantless electronic surveillance by executive branch).

[38] United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973).

[39] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III (codified as amended at 18 U.S.C. §§ 2501–2522 (2000)).

[40] 18 U.S.C. § 2518.

> other hostile acts of a *foreign power*, [2] to obtain *foreign intelligence information* deemed essential to the security of the United States, or [3] to protect national security information against *foreign intelligence activities*.[41]

The proviso's next sentence was meant to cover the President's power to deal with domestic threats to national security:

> Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States [4] against the overthrow of the Government by force or other unlawful means, or [5] against any other clear and present danger to the structure or existence of the Government.[42]

As the U.S. Supreme Court would conclude, this proviso evinced Congress's "neutrality" on the existence and scope of the President's inherent power to authorize warrantless electronic surveillance for national security purposes.[43] Even so, Title III has significance: By addressing surveillance for criminal law enforcement purposes while not addressing surveillance for national security purposes, Title III implies that the two sets of purposes differ.[44] Title III's proviso is also significant for its separation of foreign threats to national security from domestic threats.

In the face of Congress's agnosticism on the President's power to conduct electronic surveillance for national security purposes, the Court addressed the matter in *United States v. United States District Court for the Eastern District of Michigan*, known as the *Keith* case.[45]

---

[41] Title III, § 802, 82 Stat. 214 (1968) (bracketed numerals and italics added), *repealed by* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 201(c), 92 Stat. 1797.

[42] *Id.* (bracketed numerals added); *see also Foreign Intelligence Surveillance Act of 1978: Hearings Before the Subcomm. on Intelligence and the Rights of Americans of the Senate Select Comm. on Intelligence*, 95th Cong. 266 (1978) (reproducing findings of Church Committee, Final Report, Book II, at 188) (describing second sentence of Title III proviso as "deal[ing] with domestic intelligence interests," whereas first sentence of proviso "related to foreign intelligence and counterintelligence matters") [hereinafter *Senate Intelligence Hearing on FISA*].

[43] United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 308 (1972); *see also* Katz v. United States, 389 U.S. 347, 359 n.23 (1967) (reserving the issue, in a case involving electronic surveillance of domestic crime, "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security").

[44] *See* S. REP. NO. 90-1097, at 94 (1968) (recognizing "a distinction between the administration of domestic criminal legislation . . . and the conduct of foreign affairs").

[45] 407 U.S. 297 (1972). Damon J. Keith was the judge who decided the case in the federal district court. *Id.* at 298. After he ordered the government to disclose information gathered by electronic surveillance, the government sued him for a writ of mandamus in the court of appeals. *Id.* at 301. This procedural history and the case's generic official title probably explain why it is known as the *Keith* case.

The *Keith* Court ended up dealing only with the President's power to conduct electronic surveillance of domestic, not foreign, threats to national security. Specifically, the Court held in *Keith* that the Fourth Amendment generally requires the government to get judicial approval before it can conduct electronic surveillance of a domestic threat to national security.[46] (*Keith* involved a domestic organization's plan to bomb a CIA office in Ann Arbor, Michigan.[47]) The Court emphasized, however, that although the Fourth Amendment generally requires prior judicial approval for electronic surveillance of domestic threats to national security, the Fourth Amendment might otherwise require less stringent procedures and standards for that kind of surveillance than Title III required for surveillance of "ordinary crime."[48] Thus, the *Keith* Court distinguished between surveillance for information related to domestic threats to national security and surveillance for information of ordinary crime. The *Keith* Court drew a further distinction—one between surveillance related to domestic threats to national security and surveillance related to foreign threats to national security. The Court drew this latter distinction to limit its holding. The Court said, "We have not addressed, and express no opinion as to, the issues which may be involved with respect to the activities of foreign powers or their agents."[49] Despite – indeed, partly because of – that disclaimer, the *Keith* opinion suggests that the Fourth Amendment varies in stringency, requiring the most strict procedures and standards for electronic surveillance of "ordinary crime" (the subject of Title III); less strict procedures and standards – which nonetheless generally include prior judicial approval – for electronic surveillance for information related to domestic threats to national security (the subject of *Keith* itself); and the least strict procedures and standards for electronic surveillance for foreign threats to national security (the context as to which the *Keith* Court expressly reserved decision).

The D.C. Circuit extended *Keith*, thereby restricting the government's power to conduct warrantless electronic surveillance in the name of national security, in *Zweibon v. Mitchell*.[50] *Zweibon* arose

---

[46] *Id.* at 314–21.

[47] *Id.* at 299–300.

[48] *Id.* at 322; *see also id.* at 323 (stating that Congress could prescribe procedures for electronic surveillance of domestic security threats as long as "they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens").

[49] *Id.* at 321–22.

[50] 516 F.2d 594 (D.C. Cir. 1975) (en banc).

from the government's warrantless electronic surveillance of the Jewish Defense League (JDL).[51] The surveillance had been prompted by JDL activities, both peaceful and violent, against the Soviet Union's diplomatic and cultural installations in the United States.[52] The government asserted that those activities threatened Soviet-U.S. relations and could lead to Soviet retaliation against U.S. citizens in the Soviet Union.[53] Therefore, the government argued, the warrantless surveillance was a reasonable measure to address threats posed to the United States by a foreign power (the Soviet Union). The en banc D.C. Circuit rejected this argument.[54] A majority held that the surveillance violated the Fourth Amendment. Two members of the majority (Judges Wilkey and MacKinnon), each writing separately, concluded that, even if the Fourth Amendment's warrant requirement has a "'foreign affairs' exemption," the exemption "encompass[es] only surveillances on foreign agents and those in criminal collaboration with a foreign power," and JDL did not fall into either category.[55] A plurality of four judges went further, stating in dicta that, "absent exigent circumstances, *all* warrantless electronic surveillance is unreasonable and therefore unconstitutional."[56] Thus, the *Zweibon* court held that the warrantless surveillance in that case violated the Fourth Amendment, even though it related to "the activities of foreign powers or their agents,"[57] because the targets of

---

[51] *Id.* at 605–06.

[52] *Id.* at 607–09.

[53] *Id.*

[54] Eight judges constituted the en banc court in *Zweibon*. Four judges—in an opinion by Judge Skelly Wright for himself and Chief Judge Bazelon and Judges Leventhal and Spottswood Robinson—held that the surveillance violated both the Fourth Amendment and Title III. *See id.* at 615–70. Two judges, Judges McGowan and Robb, concluded that the surveillance violated Title III, without reaching the constitutional issue. *Id.* at 681–89. Two other judges, Judges Wilkey and MacKinnon, concluded that the surveillance violated the Fourth Amendment but not Title III. *Id.* at 689–707.

[55] *Id.* at 700 (Wilkey, J., concurring in part and dissenting in part); *see also id.* at 706 (MacKinnon, J., concurring in part and dissenting in part) ("At least in the case of collaborators or agents of a foreign power, I believe the national interest requires that the President be free to engage in his information gathering functions without the burden of obtaining prior judicial approval.").

[56] *Id.* at 614 (emphasis added); *see also id.* at 651 ("[O]ur analysis would suggest that, absent exigent circumstances, *no* wiretapping in the area of foreign affairs should be exempt from prior judicial scrutiny, irrespective of the justification for the surveillance or the importance of the information sought."). The plurality hesitantly agreed with the two other judges who made up the majority that the Fourth Amendment requires a warrant for electronic surveillance "at least in situations where the subject of the surveillance is a domestic organization that is not the agent of or acting in collaboration with a foreign power." *Id.* at 614. *But cf. id.* at 654 ("[W]e doubt that an exception to the warrant requirement should be created even for the activities of foreign agents or collaborators.").

[57] United States v. United States District Court for the Eastern District of Michigan, 407

the surveillance were not themselves foreign powers or foreign agents.

Zweibon influenced the enactment of the FISA.[58] *Zweibon* led the Department of Justice to fear that the D.C. Circuit would invalidate all warrantless electronic surveillance for foreign intelligence information.[59] This fear, in turn, led the Department to collaborate with Congress on drafting legislation to authorize electronic surveillance for foreign intelligence information.

Additional pressure for legislation arose from public revelations of the government's ongoing, widespread surveillance of U.S. citizens and organizations in the name of national security.[60] Many abuses became public through the Watergate scandal and the Church Committee reports.[61] The abuses included two forms particularly

---

U.S. 297, 321–22 (1972).

[58] *See, e.g.*, Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 805 (1989).

[59] *See* E-Mail from William F. Funk, Professor of Law, Lewis & Clark Law School, to Richard H. Seamon (Oct. 2, 2004) (describing *Zweibon* as a "critical development" because it "in effect signaled that the D.C. circuit would hold surveillances even of foreign powers unconstitutional absent a judicial warrant") (on file with author); *see also Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearing on S. 3197 before the Subcomm. on Intelligence and the Rights of Americans of the Senate Select Comm. on Intelligence*, 94th Cong., 2d Sess. 77 (1976) (testimony of Attorney General Edward Levi) (citing *Zweibon* as evidence of need for legislation "to achieve a coherence, stability and clarity in the law and practice that alone can assure necessary protection of the Nation's safety and of individual rights"). As discussed below, other courts—both before and after *Zweibon*—concluded that the Fourth Amendment allows the government to conduct warrantless electronic surveillance for the purpose of obtaining foreign intelligence information. *See infra* notes 174–209. The D.C. Circuit's decision nonetheless carried great weight because those challenging the surveillance would often be able to sue in the District of Columbia. For example, *Zweibon* was a civil action by members of the JDL against the Attorney General John Mitchell "and various former subordinates of his" in the FBI. *See* Zweibon v. Mitchell, 516 F.2d at 675 (Bazelon, J., concurring in part and dissenting in part).

[60] *See, e.g.*, S. REP. NO. 95-604, at 7 (1978) (referring to revelations of abuses in electronic surveillance); H.R. REP. NO. 95-1283, Pt. I, at 21 (1978) ("In the past several years, abuses of domestic national security surveillances have been disclosed."); *id.* at 111 (dissenting views on H.R. 7308) ("No one can deny that abuses of electronic surveillance have taken place in the past under the claim of 'national security.'").

[61] *See, e.g.*, S. REP. NO. 95-604, at 7 (1978) (stating that abuses in electronic surveillance "were initially illuminated in 1973 during the investigation of the Watergate break-in" and that additional abuses had been brought to light by the Church Committee); S. REP. NO. 95-701, at 9 (1978) (stating that Church Committee report "provided firm evidence that foreign intelligence electronic surveillance involved abuses and that checks upon the exercise of those clandestine methods were clearly necessary"); *Senate Intelligence Hearing on FISA*, *supra* note 42, at 9 (reproducing Additional Views of Sen. Biden on S. 3197, 94th Cong. (1977)) ("Congress is on notice of the myriad of [surveillance] abuses . . . in the course of the Watergate matter."); *id.* at 110 (prepared statement of John Shattuck and Jerry Berman, ACLU):

> This legislation has been proposed for the same reasons that this new Intelligence Committee was constituted: the recognition, in the wake of Watergate and

relevant to the FISA. One form concerned the collection of information; the other concerned the use of the information that had been collected. As to the first type of abuse, the government collected "enormous amounts of personal and political information serving no legitimate governmental interest."[62] It collected such personal and political information from, among others, civil rights leaders such as Martin Luther King, Jr., and domestic political organizations such as the Women's Liberation Movement.[63] The second form of abuse concerned the use to which the information was put. Not only the political and personal information collected, but also even the information that potentially had a valid use for national security purposes, was used by the FBI and government officials for stifling domestic dissent, giving the incumbent Presidents politically useful information about their opponents, and enhancing the FBI's power and position in the bureaucracy.[64] For example, the FBI peddled surveillance information to Presidents and members of Congress

---

> revelations of massive illegal programs conducted by the FBI, CIA, NSA and other U.S. intelligence agencies, that the Congress must . . . enact legislation . . . which insure[s] that intelligence activities will no longer violate the civil and constitutional rights of Americans.

Id. The Church Committee was chaired by Senator Church of Idaho. The House of Representatives also held hearings chaired by Representative Otis Pike, though its final report was not officially published. *See* James R. Coben, *Gollum, Meet Sméagol: a Schizophrenic Rumination on Mediator Values Beyond Self-determination and Neutrality*, 5 CARDOZO J. CONFLICT RESOL. 65, 65 (2004) (stating that Pike report never official published).

[62] *Senate Intelligence Hearing on FISA*, *supra* note 42, at 261 (reproducing "Major Finding" of Church Committee, Final Report, book II, at 183); *see also* S. REP. NO. 95-604, at 8 (1978) (quoting Church Committee Report of electronic surveillance under "vague and elastic standards" that had produced "vast amounts of information—unrelated to any legitimate government interest—about the personal and political lives of American citizens").

[63] *Senate Intelligence Hearing on FISA*, *supra* note 42, at 271, 277 (1978) (reproducing Church Committee, Final Report, book II, at 193, 199); *see also* S. REP. NO. 95-604, at 29 (1978) (discussing investigation of Dr. King).

[64] *See, e.g.*, *Intelligence Activities: Hearings before the Senate Select Comm. to Study Governmental Operations with respect to Intelligence Activities, Volume 6, Federal Bureau of Investigation*, 94th Cong., 1st Sess. 164 (1975) (describing FBI surveillance of Republican leader Anna Chennault that was apparently requested by President Johnson for political purposes but that also reflected suspicion of activities that might have violated Foreign Agents Registration Act and Neutrality Act) [hereinafter cited as *Church Committee Hearing on the FBI*]; *Intelligence Activities and the Rights of Americans*, book II, S. REP. NO. 94-755, at 64–65, 200 n.85, 233–34 (1976) (describing FBI surveillance requested by President Kennedy of possibly illegal foreign pressure on Congressional sugar quota deliberations, which were "arguably related to 'foreign intelligence'" but also "potentially useful to the Kennedy administration for purely political purposes") [hereinafter cited as *Church Committee Final Report*]; *id.* at 119–20 (describing President Johnson's political use of FBI surveillance of foreign officials); *see also Senate Intelligence Hearing on FISA*, *supra* note 42, at 100 (prepared statement of Prof. Christopher Pyle) (summarizing political uses of wiretap evidence revealed in Church Committee report).

about political opponents to curry favor for FBI pet projects and funding.[65] In sum, the Church Committee Reports showed that, in the name of national security, government officials were collecting information that could not fall within the most generous definition of "national security information" and using it, as well as potentially legitimate national security information, for purposes unrelated to national security.

Congress enacted the FISA to curb such abuses by regulating the executive branch's use of electronic surveillance.[66] Congress did not deny the President's inherent power to conduct electronic surveillance for national security purposes.[67] Instead, Congress took the position that even if the President had such power, Congress could regulate that power by prescribing reasonable procedures for its exercise.[68] Neither the Ford Administration nor the Carter Administration

---

[65] *Senate Intelligence Hearing on FISA*, *supra* note 42, at 128 (testimony of Morton Halperin, Center for National Security Studies) ("Presidents have asked the FBI what it knew about the views of U.S. Senators, for example, on the Vietnam war."); *id.* at 289 (reproducing portion of Church Committee report describing instances when FBI disseminated intelligence information "to entrench the Bureau's own position in the political structure, regardless of which party was in power at the time"); *id.* at 289–90 ("Presidents and White House aides have asked the FBI to provide political or personal information on opponents and critics, including 'name checks' of Bureau files. They have also asked the Bureau to conduct electronic surveillance . . . of such persons.") (footnote omitted); *id.* at 300–03 (describing other instances of FBI's use of surveillance information to curry favor).

[66] *See, e.g.*, 124 CONG. REC. 10,887 (1978) (statement of Sen. Kennedy) ("The abuses of recent history sanctioned in the name of national security and documented in detail in the Church committee highlight the need for more effective statutory controls and congressional oversight."); *id.* at 10889 (statement of Sen. Bayh) ("[T]his bill is required absolutely, unqualified[ly], because of certain misconduct and abuse which are almost unbelievable"); S. REP. NO. 95-604, at 7 (1978) ("This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused."); *Senate Intelligence Hearing on FISA*, *supra* note 42, at 4 (statement of Sen. Huddleston) ("The abuses which were discovered in the area of warrantless wiretaps made clear the necessity for legislative action.").

[67] The FISA repealed the Title III proviso that addressed the President's supposed "inherent" power and that was discussed in *Keith*. Pub. L. No. 95-511, § 201(c), 92 Stat. 1797. The repeal was meant to dispel the misperception that the proviso ratified the existence of such power. *See, e.g.*, S. REP. NO. 95-604, at 6 (1978).

[68] *See, e.g.*, S. REP. NO. 95-604, at 16 (1977) ("The basis for this legislation is the understanding—concurred in by the Attorney General—that even if the President has an 'inherent' constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance."); H.R. REP. NO. 95-1283, Pt. I, at 24 (1978) ("[E]ven if the President has the inherent authority in the absence of legislation to authorize warrantless electronic surveillance for foreign intelligence purposes, Congress has the power to regulate the conduct of such surveillance by legislating a reasonable procedure, which then becomes the exclusive means by which such surveillance may be conducted.").

opposed congressional regulation of Executive power.[69] Indeed, representatives from both administrations supported the legislation, despite awareness that it restricted executive power.[70] Executive support seemed to reflect a desire, in the wake of Watergate and the Church Committee reports, to regain credibility for national security surveillance, and, in the wake of court decisions such as *Zweibon*, to secure a constitutionally solid statutory foundation for such surveillance.[71] The resulting legislation is discussed next.

B. FISA

Cognizant of *Keith's* delineation of surveillance involving "foreign powers" and their "agents,"[72] the 95th Congress used those very terms in the FISA.[73] The FISA authorized the federal government,

---

[69] *See, e.g.*, 124 CONG. REC. 10,887 (1978) (statement of Sen. Kennedy) (observing that S.1566, 95th Cong., had support of Ford and Carter administrations).

[70] S. REP. NO. 95-604, at 16 (1977) (Congress's assertion in the FISA of power to regulate the President's authorization of electronic surveillance for foreign intelligence purposes was "concurred in by the Attorney General"); H.R. REP. NO. 95-1283, pt. 1, at 24 (1978) (Congress's determination that it had power by legislation to regulate President's use of electronic surveillance for foreign intelligence purposes "has been supported by two successive Attorneys General"); *Foreign Intelligence Surveillance Act of 1977: Hearings before the Senate Subcomm. on Criminal Laws and Procedures of the Comm. on the Judiciary* [hereinafter *Senate Judiciary Hearing on FISA*], at 56 (statement of Adm. Stansfield Turner, Director of CIA) ("Clearly this bill will inhibit the collection of foreign intelligence to some degree. However, in my view that is worth the increase in credibility and increased assurance of the people of the United States in their intelligence operations and in the protection of their rights."); *id.* at 98 (testimony of Morton Halperin) (stating that under proposed legislation "there has been a substantial reduction in the Presidential power"); *Foreign Intelligence Electronic Surveillance: Hearings before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence* [hereinafter *House Judiciary Hearing on FISA*], at 38 (testimony of Attorney General Griffin Bell) ("[W]e have had two President's [sic] in a row who are willing to cede power" to conduct electronic surveillance for foreign intelligence); *Senate Intelligence Hearing on FISA*, at 12 (prepared statement of Attorney General Griffin Bell) (expressing his awareness of "the abuses of the past" and his support for bill); *id.* at 25 (testimony of Attorney General Griffin Bell) ("While it may seem strange for me to be indicating that we want to give up power that we now have, we do."); *id.* at 40 ("[W]e're willing to give up this power.").

[71] *See, e.g.*, 124 CONG. REC. 10,889 (1978) (statement of Sen Garn) (stating that "uncertainty and ambiguity" in the law had caused there to be "very few authorizations for electronic surveillance of U.S. citizens for foreign intelligence purposes during the last 5 years").

[72] United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 321–22 (1972).

[73] Pub. L. No. 95-511, 92 Stat. 1783 (1978); FISA's enactment by the 95th Congress in 1978 followed several failed attempts to enact similar legislation in prior Congresses. *See* 124 CONG. REC. 10,887 (1978) (statement of Sen. Kennedy) (referring to "the ongoing 10-year debate to regulate foreign intelligence electronic surveillance"); S. REP. NO. 95-604, at 7 (1978) (citing prior bills regulating electronic surveillance and prior hearings on those bills); H.R. REP. NO. 95-1283, pt. 1, at 13 (1978) (reporting that bills requiring a warrant for foreign intelligence electronic surveillance "had been introduced in the House and Senate each year since 1973"). The FISA was based on S.1566, 95th Cong., a direct

with prior judicial approval, to conduct electronic surveillance of "foreign powers" and "agents of foreign powers" for "foreign intelligence information." [74] Three aspects of the FISA are especially important for understanding the subject of this article – the extent to which FISA surveillance can be used for prosecutorial purposes. The relevant aspects are: (1) how the government applies under the FISA for a judicial order authorizing electronic surveillance; (2) what a court must find to issue such a FISA surveillance order; and (3) what uses the government can make of the information obtained under the order. This examination is necessarily detailed, as it lays groundwork for this article's ultimate conclusion that all significant precedent has misunderstood the extent to which FISA can be used for prosecutorial purposes.

1. Applications for FISA Surveillance Orders

An application for a FISA surveillance order requires Attorney General approval.[75] Once approved, the application goes to a court created by the FISA called the Foreign Intelligence Surveillance Court.[76] That court consists of eleven federal district judges selected by the Chief Justice for seven-year terms.[77] The court's proceedings are ex parte.[78] Since the government is the only party to the proceeding, a court order granting the government's application without modification is not subject to direct review.[79] In contrast, a

---

forerunner of which was S. 3197, 94th Cong. (1976). *See* S. REP. NO. 95-604, at 3 (1978). The House version of S.1566 that was reported in the 95th Congress was H.R. 7308. *See generally* H.R. REP. NO. 95-1283, pt. 1 (1978) (report on H.R. 7308).

[74] As amended after 1978, the FISA was expanded to authorize judicial approval of physical searches, see 50 U.S.C. §§ 1821-1829 (2000), pen registers and trap-and-trace devices, see *id.* §§ 1841–1846, and documents and other tangible things, see *id.* §§ 1861–1862. This article focuses on electronic surveillance.

[75] *See id.* § 1804(a)(2); § 1805(a)(2).

[76] *See id.* § 1803(a).

[77] *See id.*

[78] *See id.* ("Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if" the judge makes the prescribed findings.); *cf.* FED. R. CRIM. P. 4(a) and 41(d), (g) & (h) (providing for *ex parte* issuance of arrests warrants and search warrant and for post-execution challenges to searches conducted under warrants).

[79] An order granting a government application for an order approving electronic surveillance may not conclusively establish the legality of the ensuing surveillance. If the government obtains information that it seeks to use against someone in a later proceeding, including a criminal proceeding, the person can challenge the legality of the surveillance. *See* 50 U.S.C. § 1806(b)–(g) (2000). If the evidence is not so used, however, the surveillance order is, as a practical matter, conclusive of the surveillance's legality. Indeed, the target of the surveillance may never find out the surveillance occurred. *But cf.* 50 U.S.C. § 1806(j)(3) (2000) (providing for notice to target when court fails to approve emergency electronic surveillance); *id.* § 1825(b) & (j) (2000) (providing for notice to

court order denying the government's application in whole or in part is subject to review, at the government's instance, by a second court created by the FISA, the United States Foreign Intelligence Surveillance Court of Review.[80] This article hereafter refers to the two courts created by the FISA, individually, as the FISA Trial Court and the FISA Court of Review (or simply "Court of Review") and, collectively, as "the FISA courts."

The application must identify or describe "the target" of the proposed surveillance.[81] The application must also include a statement describing the basis for the applicant's belief that:

> (A) the target . . . is a foreign power or an agent of a foreign power; and
>
> (B) each of the facilities or places at which the [proposed] electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.[82]

Thus, FISA surveillance may cover only facilities or places used or to be used by a "foreign power" or an "agent of a foreign power."[83] This makes the definitions of "foreign power" and "agent of a foreign power" critical to the scope and permissible purposes of FISA surveillance.

Of relevance in this post-9/11 era, the term "foreign power" covers both official and unofficial foreign entities, including terrorist groups like al Qaeda. "Foreign power" means:

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

---

target of physical searches authorized under FISA).

[80] *Id.* § 1803(b).

[81] *Id.* § 1804(a)(3).

[82] *Id.* §1804(a)(4).

[83] *Id.* § 1804(a)(4)(B).

> (6) an entity that is directed and controlled by a foreign government or governments.[84]

For our purposes, this definition of "foreign power" deserves attention mostly because it controls the meaning of "agent of a foreign power."[85]

The definition of "agent of a foreign power" distinguishes "United States persons" from everyone else.[86] The term "United States person" includes U.S. citizens and permanent resident aliens.[87] The FISA specially protects the privacy interests of U.S. persons.[88] A "U.S. person" can be an "agent of a foreign power" only if he or she:

> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in . . . (A), (B), or (C) or knowingly conspires . . . to engage in [such] activities . . . .[89]

Someone who is not a "United States person" can be an "agent of a foreign power" under additional circumstances, which need not be

---

[84] *Id.* § 1801(a); *see, e.g.*, United States v. Falvey, 540 F. Supp. 1306, 1310 (E.D.N.Y. 1982) (contending that Irish Republican Army was "foreign power").

[85] 50 U.S.C. § 1801(b) (defining "[a]gent of a foreign power" by references to actions for or on behalf of a "foreign power").

[86] *Compare id.* § 1801(b)(1) (defining "[a]gent of a foreign power" for "any person *other than a United States person*") (emphasis added), *with id.* § 1801(b)(2) (defining "[a]gent of a foreign power" for "any person").

[87] *Id.* § 1801(i).

[88] *See, e.g.*, S. REP. NO. 95-701, at 19 (1978) (providing rationale for this discrimination).

[89] 50 U.S.C. § 1801(b)(2).

detailed here.[90] In general, this article focuses on FISA surveillance of foreign agents who are U.S. persons (who will sometimes be referred to as "U.S. person-foreign agents"). U.S. persons are the ones whom the wall was created to protect.[91]

In addition to explaining why the applicant believes that the proposed surveillance will target facilities used or about to be used by a foreign power or foreign agent, an application for FISA surveillance must contain certifications.[92] These certifications can be made only by certain high-ranking executive branch officials involved in national security or national defense.[93] Of those officials, the Director of the FBI is the one who usually makes the certifications in applications for surveillance of U.S. persons.[94] The original FISA of 1978 required certifications by the FBI Director or other authorized official:

> (A) that the certifying official deems the information sought to be foreign intelligence information;
>
> (B) that the purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) that such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e); and
>
> (E) including a statement of the basis for the certification that—
>
> (i) the information sought is the type of foreign intelligence information designated; and

---

[90] *Id.* § 1801(b)(1).

[91] *See, e.g.*, FISA Trial Court Opinion, 218 F. Supp. 2d 611, 614 (Foreign Int. Surv. Ct. Rev. 2002) (defining "scope" of opinion as limited to U.S. persons); *see also infra* notes 227–62 and accompanying text (discussing development of internal Justice Department procedures that came to be known as "the wall").

[92] *See* 50 U.S.C. § 1804(a)(7) (Supp. 2001).

[93] *See id.* (providing for certifications to be made by "the Assistant to the President for National Security Affairs [i.e., the National Security Adviser] or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate"); *see also* Exec. Order No. 12,139, 3 C.F.R. 398 (1979), *reprinted in* 50 U.S.C. § 1801 app. at 275 (2000) (designating officials authorized to make FISA certifications).

[94] *See In re* Sealed Case, 310 F.3d 717, 723 (Foreign Int. Surv. Ct. Rev. 2002) (noting that certifications required by the FISA are "typically" made by the FBI Director); FISA Trial Court Opinion, 218 F. Supp. 2d at 619–20 (describing FISA as requiring "that the FBI Director certify" to certain things).

> (ii) such information cannot reasonably be obtained by normal investigative techniques . . . .[95]

These certification requirements include the key provisions discussed in this article. Most important is the second certification requirement, about the "purpose" of the proposed surveillance, § 1804(a)(7)(B). As discussed below, lower courts relied on this "purpose" provision in adopting the "primary purpose" test.[96] Furthermore, the Patriot Act amended the purpose provision by changing the phrase "the purpose" to "a significant purpose."[97]

The certification requirements just reproduced reflect that a third key term – in addition to the terms "foreign power" and "agent of a foreign power" – is "foreign intelligence information." The FISA provides a two-part definition of "foreign intelligence information," reflecting two commonly accepted categories of such information:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.[98]

Subsection (1) of this definition describes three types of what is commonly called "counterintelligence" or "protective intelligence."[99]

---

[95] FISA § 104(a)(7) (1978).

[96] *See infra* notes 210–23 and accompanying text.

[97] *See infra* notes 287–301 and accompanying text.

[98] 50 U.S.C. § 1801(e)(2000); *see also* 124 CONG. REC. 10,890 (1978) (statement of Sen. Bayh) (describing two types of foreign intelligence information covered by FISA); S. REP. NO. 95-701, at 9 (1978) (stating that definition of foreign intelligence information covers "two broad types of [government's] intelligence requirements").

[99] *See, e.g.*, S. REP. NO. 95-701, at 9 (describing "counterintelligence" as designed "to

This category of foreign intelligence information bears on protecting the United States against—i.e., countering—foreign threats. Subsection (2) of the definition identifies two types of what is commonly called "positive" intelligence, "affirmative" intelligence, "pure" intelligence, or just plain "intelligence."[100] This category tends to be more diffuse—less event-specific—than the first type of foreign intelligence information ("counter" or "protective" intelligence).[101] That is why it is usually FISA surveillance for counterintelligence—rather than FISA surveillance for plain intelligence—that has the potential for producing evidence of criminal activity and, hence, the potential for breaching "the wall" between foreign intelligence and law enforcement.[102]

In addition to identifying the target and making certifications, the government's application for a FISA surveillance order must include "proposed minimization procedures."[103] The FISA provisions on minimization procedures are discussed in more detail in a later subsection.

2. Judicial Approval of FISA Surveillance Orders

An application for a FISA surveillance order is made to one of the eleven federal district judges appointed by the Chief Justice to serve on the FISA Trial Court.[104] The judge must decide whether to grant the application and issue an order approving electronic surveillance[105]

---

protect" against certain foreign threats).

[100] *In re* Sealed Case, 310 F.3d 717, 723 n.9 (Foreign Intelligence Surveillance Court of Review 2002); *see also* Exec. Order No. 12,333, 3 C.F.R. 211 (1981), *reprinted in* 50 U.S.C. § 401 app. at 61–62 (2000).

[101] *See, e.g.*, S. REP. NO. 95-701, at 9:

> The electronic surveillance authorized and regulated by this bill is designed to satisfy two broad types of intelligence requirements. First, it provides a means for the collection of 'positive' foreign intelligence to enable the Government to understand and assess the capabilities, intentions, and activities of foreign powers. Second, it supplies a technique for use in foreign counterintelligence investigations to protect against clandestine intelligence activities, sabotage, and terrorism by or on behalf of foreign powers.

Id.

[102] *See, e.g.*, *In re* Sealed Case, 310 F.3d at 727 ("[T]he type of foreign intelligence with which we are concerned is really counterintelligence . . . ."); Hill, *Joint Inquiry Staff Statement*, *supra* note 3, at 23 ("As the 1980s began, the law enforcement and intelligence communities worked together most often in the context of counterintelligence investigations and counternarcotics programs."); *see also* 9/11 COMM'N REPORT, *supra* note 2, at 424 ("Counterterrorism investigations in the United States very quickly become matters that involve violations of criminal law and possible law enforcement action.").

[103] 50 U.S.C. § 1804(a)(5)(2000); *see infra* notes 139–59 (describing provisions on minimization procedures).

[104] 50 U.S.C. § 1803(a)(Supp. 2001).

[105] *Id.* § 1805.

based on five "necessary findings"[106]:

> (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
>
> (2) the application has been made by a Federal officer and approved by the Attorney General;
>
> (3) on the basis of the facts submitted by the applicant there is probable cause to believe that—
>
> (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and
>
> (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (4) the proposed minimization procedures meet the definition of minimization procedures under section 1804(h) of this title; and
>
> (5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.[107]

The first two "necessary findings" seldom cause much trouble.[108] The rest need more attention.

The third necessary finding comes closest to traditional probable cause and, in the process, makes FISA surveillance orders akin— if not equivalent—to Fourth Amendment "warrants." To discuss them out of order: Necessary finding 3(B)—probable cause that the

---

[106] 50 U.S.C. § 1805(a) (2000) (title of subsection (a) is "Necessary findings").

[107] *Id.* § 1805(a). Section 1805(a)(5), which is quoted in the text accompanying this note, refers to "information furnished under section 1804(d)." Section 1804(d) authorizes the FISA judge to "require the applicant to furnish such other information as may be necessary to make the determinations required by section 1805 of this title." *Id.* § 1804(d).

[108] The President has authorized the Attorney General to approve FISA applications. Exec. Order No. 12,333, 3 C.F.R. 212 (1981), *reprinted in* 50 U.S.C. § 401 app. at 62 (2000). The Attorney General, in turn, has authorized FISA applications to be prepared and submitted under the supervision of the Counsel for Intelligence Policy in the Office of Intelligence Policy and Review ("OIPR"). 28 C.F.R. § 0.33b (2004); *see also* United States Attorneys' Manual, § 12.106 (stating that OIPR "prepares certifications and applications" for FISA surveillance).

surveilled facilities are used or will be used by the target—addresses one of the particularity requirements in the Fourth Amendment.[109] The Fourth Amendment requires a warrant to "particularly describ[e] the place to be searched."[110] The "place to be searched" by electronic surveillance may be a physical place or a communications facility.

Necessary finding 3(A)—probable cause that the target is a foreign power or agent of a foreign power[111]—can overlap with a finding of criminal or potentially criminal conduct as applied to U.S. person-foreign agents. That is because of the portion of the definition of "agent of a foreign power" applicable to "United States persons."[112] It was reproduced above.[113] It classifies a U.S. person as a foreign agent based on their "knowing" involvement, "for or on behalf of a foreign power," in (1) "'clandestine intelligence gathering activities' [that] involve or may involve violations of Federal criminal law";[114] (2) "other clandestine intelligence activities," "pursuant to the direction of an intelligence service or network of a foreign power," "which . . . involve or are about to involve a violation of the criminal statutes of the United States"; (3) "sabotage or international terrorism [as defined elsewhere in the FISA[115]] . . . or activities that are in preparation therefor"; (4) entering or remaining in the United States "under a false or fraudulent identity"; or (5) aiding or abetting, or conspiring to engage in, any of the first three categories of activities listed in this sentence. Thus, to find probable cause that a U.S. person is an "agent of a foreign power," the judge usually must find evidence of conduct that is a crime or is likely to be a crime. This is not invariably true, however, because the definition of "agent of a foreign power" includes some conduct, such as entering or remaining in the United States under a false or fraudulent identity, that is not always a crime, even when done on behalf of a foreign power.[116]

---

[109] *See* H.R. REP. NO. 95-1283, pt. 1, at 81 (1978) (tracing this finding to Fourth Amendment's particularity requirement).

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

[111] 50 U.S.C. § 1805(a)(3)(A).

[112] *Id.* § 1801(b)(2).

[113] *See supra* note 89 and accompanying text.

[114] *See* S. REP. NO. 95-701, at 21 (1978) ("It is anticipated that most of the persons under surveillance under [the provision defining agent of a foreign power to include U.S. persons involved in clandestine intelligence gathering] will be violating the criminal espionage laws . . . ."); H.R. REP. NO. 95-1283, pt. 1, at 38 (1978) ("It is anticipated that most clandestine intelligence gathering activities will constitute a violation of the various federal criminal laws aimed at espionage . . . .").

[115] *See* 50 U.S.C. § 1801(c) (defining "[i]nternational terrorism") and § 1801(d) (defining "[s]abotage").

[116] *See In re* Sealed Case, 310 F.3d 717, 723 n.10 (Foreign Int. Surv. Ct. Rev. 2002). *But*

The fourth "necessary finding" for issuance of a FISA surveillance order ensures the adequacy of the minimization procedures proposed in the application for the order.[117] Like necessary finding 3(B) (probable cause that the facilities to be surveilled are used or are about to be used by the target), the necessary finding about minimization procedures reflects one of the particularity requirements in the Fourth Amendment.[118] The Fourth Amendment requires a warrant to "particularly describ[e] the . . . things to be seized."[119] This requirement, as applied to physical searches, prohibits an official with a warrant from indiscriminately rummaging through a person's belongings.[120] As applied to electronic surveillance, it prohibits the government from collecting and keeping every scrap of information acquired through the surveillance, including irrelevant (but potentially embarrassing or intimate) personal or political information.[121] Minimization procedures aim to limit such indiscriminate conduct.

The fifth "necessary finding" concerns the certifications and statements that a high-level executive official with intelligence responsibilities must make in the application.[122] The judge must ensure that the application indeed contains those certifications and statements.[123] Furthermore, if the proposed target is a U.S. person, the judge must determine that the certifications and statements are not "clearly erroneous."[124] For this article, the most important certifications subject to judicial review under this standard are that: (1) the information to be obtained is "foreign intelligence information"; and (2) "the purpose" (under the original FISA) or "a significant purpose" (under the FISA as amended by the Patriot Act) of the proposed surveillance "is to obtain foreign intelligence information."[125] Also important are the requirements that the certifying official designate the type of information sought, using the typology of the FISA's definition of "foreign intelligence

---

cf. id. at 736 (apparently amending definition of "foreign intelligence crime" to include "ordinary crimes . . . inextricably intertwined with foreign intelligence crimes").

[117] *See* 50 U.S.C. § 1805(a)(4).

[118] *See* H.R. REP. NO. 95-1283, pt. 1, at 81 (1978) (tracing this finding to the Fourth Amendment's particularity requirement).

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

[120] *See, e.g.*, Andresen v. Maryland, 427 U.S. 463, 480 (1976).

[121] *See* Berger v. New York, 388 U.S. 41, 57–59 (1967).

[122] *See* 50 U.S.C. § 1805(a)(5).

[123] *See id.*

[124] *Id.*

[125] 50 U.S.C. § 1804(a)(7)(A) & 50 U.S.C. § 1804(a)(7)(B)(Supp. 2001).

information,"[126] and state the basis for his or her certification that the information is the type of foreign intelligence information designated.[127] All of these add up to a requirement that the purpose (or a significant purpose) of proposed surveillance of a foreign power or its agent be to obtain one of the three types of counterintelligence or one of the two types of (plain) intelligence identified in the FISA's definition of "foreign intelligence" information.[128]

As discussed above, the definition of "agent of a foreign power," as applied to U.S. persons, causes FISA surveillance orders targeting such persons often to be based on evidence of crime. Similarly, the definition of "foreign intelligence information" can cause FISA surveillance orders to be based on a likelihood that surveillance will reveal evidence of crime, even if the target herself is not involved in crime. For example, surveillance of a target may reveal information that qualifies as "foreign intelligence information" because it is evidence of a crime, such as international terrorism, by a third party, but not by the target.[129] The bottom line is that the text of the FISA, as concerns U.S. persons, defines key terms and prescribes "necessary findings" in ways that can—but do not necessarily—lead to the issuance of surveillance orders that are (1) based on evidence of crime; and (2) likely to produce more evidence of crime.

3. The Government's Intended and Actual Use of FISA-Acquired Information

Three sets of provisions bear on the government's intended and actual use of information obtained under a FISA surveillance order. Two of those groups have already been briefly introduced: the provisions requiring a certification of the "purpose" of proposed surveillance;[130] and the provisions on minimization procedures.[131] The third group is found in Section 1806 of the FISA, which is entitled "Use of information." Each group is separately discussed next.

---

[126] 50 U.S.C. § 1804(a)(7)(D) (2000).

[127] *Id.* § 1804(a)(7)(E)(i).

[128] *See supra* note 98 and accompanying text (reproducing FISA definition of "foreign intelligence information").

[129] *Cf.* Zurcher v. Stanford Daily, 436 U.S. 547, 554–67 (1978) (holding that Fourth Amendment does not require special showing for search of premises of people who are not reasonably suspected of involvement in crime being investigated).

[130] *See supra* notes 95–97 and accompanying text.

[131] *See supra* notes 107, 117–21 and accompanying text.

a. FISA Provisions Requiring a Certification About the Purpose of Proposed Surveillance and Authorizing Limited Judicial Review of That Certification

A high-ranking official with intelligence responsibilities must certify that "the purpose" (under the original FISA) or "a significant purpose" (under the FISA as amended by the Patriot Act) of the surveillance proposed in the government's application "is to obtain foreign intelligence information."[132] The FISA judge must determine whether that certification is "clearly erroneous" if the target of the proposed surveillance is a U.S. person.[133] Consideration of these aspects of the FISA process will illuminate whether the government can use FISA surveillance for prosecutorial purposes.

A certification about the type of thing I intend to obtain differs from a certification about how I intend to use that thing. For example, if I certify that "the purpose" of my borrowing $20,000 from you is to buy a car, I am not certifying to how I will use that car. By the same token, if a judge were authorized to determine whether my certification was clearly erroneous, she would focus on determining whether I intended to use the money to buy a car, rather than some other pricey item. The judge would have no business reviewing my purpose for wanting the car.

Accordingly, the "purpose" certification requirement in the FISA and the provision authorizing limited review of that certification do not, on their face, control the government's intended use of information obtained under a proposed FISA surveillance order. The government must certify that "a significant purpose" (formerly "the purpose") of the proposed surveillance is "to obtain foreign intelligence information."[134] The FISA judge must determine, under a clearly erroneous standard, whether the government does indeed intend to conduct the surveillance to obtain foreign intelligence information, rather than some other kind of information.[135] The government does not, however, expressly certify to how it intends to use the foreign intelligence information that it intends to obtain. It is therefore not obvious that a judge should be able to review the government's intended use of the information.

To explore that issue further, let us change the hypothetical loan

---

[132] FISA § 104(a)(7); 50 U.S.C. § 1804(a)(7)(B) (Supp. 2001).
[133] 50 U.S.C. § 1805(a)(5) (2000).
[134] 50 U.S.C. § 1804(a)(7)(B); FISA § 1804(a)(7)(B).
[135] 50 U.S.C. § 1805(a)(5).

described above. Suppose I certify that "the purpose" of my borrowing $20,000 from you is "to buy the means of transportation necessary for me to get to work." Now my certification describes the thing I want to obtain instrumentally—as having a necessary relationship to a further objective: getting to work. Considering this instrumental description of the thing that (I certify) it is my purpose to obtain, you could reasonably infer from my certification not only that I will use the money to buy a car (or other means of transportation) but also that I intend to use the car to get to work. That inference as to my intended use of the car is reasonable even though, technically, my certification did not cover my intended use of the car. Beyond what it would be reasonable for you to infer, if you required me to make the certification as a condition of lending me $20,000, you probably wanted to require me to have the intention (i.e., the purpose) of using the car to get to work. If you indeed wanted to impose such a requirement as to my intended use of the car, you might accuse me of dishonesty if—when I certified that I would use the money "to buy the means of transportation necessary for me to get to work"—I actually did not intend to use the car to get to work but, instead, intended to use it only for weekend, recreational trips (and planned to join a car pool to get to work). Alternatively or in addition, you could accuse me of using the term "necessary" too broadly, since my actual intention not to use the car to get to work disproved the car's necessity for that objective. In either event, a certification that one's purpose is to obtain a thing that is, by definition, "necessary to" achieving a specified objective implies that one intends to use the thing to attain that objective. And the requirement that one make such a certification may reflect that the party requiring the certification wants to control the certifier's intended use of the thing—specifically, wants the certifier to intend to use the thing to attain the specified objective.

The last paragraph showed that, if I certify that the purpose of my borrowing money from you is to buy the means of transportation "necessary" to get to work, you can reasonably infer—and, indeed, could be implicitly requiring—that I intend to use the car I buy with your money to get to work. Now a new point: You cannot necessarily infer that my *primary* purpose in buying the car is to get to work. I might be able honestly to assert that (1) the purpose of my loan is to buy a car; and (2) the car is necessary for me to get to work—even though my primary purpose for getting the car is for recreational road trips on the weekend. Indeed, teenagers routinely—and no doubt

sincerely and accurately—ask their parents for loans "the purpose" of which is to get the car that is "necessary" to fulfill their school and work obligations, even though use of the car for those ends is not their primary purpose for getting the car or seeking the loan. The point is that a person can certify that his or her purpose is to obtain a thing that is necessary to achieving a second goal without necessarily implying that his or her primary purpose for obtaining the thing is to achieve that second goal.

One final variation of the hypothetical loan will fully illuminate the "primary purpose" issue. The last paragraph showed that making two certifications—i.e., that (1) one's purpose is to obtain a thing; and (2) that thing is necessary to a specified objective—does not necessarily imply that one's "*primary* purpose" for obtaining the thing is to achieve the specified objective. Even so, the identity of the person who makes the certification may support a permissible inference about primary purpose. Suppose the certifier is the director of information technology for a large company. Now suppose she certifies to the company's chief financial officer that (1) she needs $2 million to upgrade the company's computers; and (2) the upgrade is necessary to protect the company's computer system from viruses and computer hackers. Surely it is permissible to infer that the director's "primary purpose" for seeking the money is to protect the company's computers from the specified threat. That inference is permissible—if not compelled— because of the link between (a) the official's duties and (b) the objective to which the thing to be obtained is necessary.

Let us return to the FISA. The original FISA required a high-ranking official with intelligence responsibilities to certify that "the purpose" of proposed surveillance was to obtain foreign intelligence information. When proposed surveillance concerned a U.S. person, the original FISA defined "foreign intelligence information" to mean information "necessary to" the United States' achievement of five purposes. The information had to be:

> (1) . . . necessary to, the ability of the United States to protect against—
>
> (A)[1] actual or potential attack or other grave hostile acts of a foreign power;
>
> (B)[2] sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C)[3] clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) . . . necessary to—

(A)[4] the national defense or the security of the United States; or

(B)[5] the conduct of the foreign affairs of the United States.[136]

By defining "foreign intelligence information" in terms of its necessary relationship to achieving these five foreign intelligence purposes, and requiring the government to certify that its purpose was to obtain "foreign intelligence information," Congress probably meant to require the government to intend to use the information for one of these five foreign intelligence purposes. (Hereafter, this article will use the term "foreign intelligence purpose" to mean one of these five purposes.) That is particularly likely considering that Congress also required the certification to be made by a high-ranking official with intelligence responsibilities (rather than, say, a law enforcement official, even one as high ranking as the Attorney General).[137] Congress presumably would have considered it dishonest, at least, for a high-ranking intelligence official to certify that "the purpose" of proposed surveillance was to obtain information "necessary to" achieving a foreign intelligence goal, if the official had no intention of using the information for that goal. To be sure, as long as the official did intend to use the information for a foreign intelligence purpose, the official could honestly certify that (1) "the purpose" (or, for that matter, "a significant purpose") of the proposed surveillance was to obtain the information; and (2) the information was necessary to achieving a foreign intelligence purpose—even if the government's "primary purpose" for seeking approval of the proposed surveillance was not to use the information for a foreign intelligence purpose but, instead, for a different purpose. Given the link between the certifying official's duties and foreign intelligence purposes, however, it would be reasonable to presume from the required certifications that the government's primary purpose for seeking the information was indeed to achieve a foreign intelligence purpose.

In short, the original FISA's "purpose" certification requirement and provision for judicial review of that certification directly address

---

[136] *Id.* § 1801(e) (bracketed numerals added).

[137] S. REP. NO. 95-604, at 45 (1978) ("The requirement that the information sought be 'foreign intelligence information' is designed to insure that a high-level official with responsibility in the area of national security, will review and . . . explain the Executive Branch determination that the information sought is in fact foreign intelligence information."); S. REP. NO. 95-701, at 51 (1978); H.R. REP. NO. 95-1283, pt. 1, at 76 (1978).

only the type of information that the government intends to obtain. These provisions can be interpreted, however, indirectly to address the government's intended use of—i.e., its purpose for seeking—that information. Specifically, the provisions imply that the government must intend to use the information for one of the five foreign intelligence purposes identified in the FISA's definition of "foreign intelligence information." The provisions do not compel—but they reasonably can be read to support—the further conclusion that the achievement of a foreign intelligence purpose must be the government's "primary purpose" for seeking the information.

An important but separate question, explored below, is whether the government can meet such a primary purpose requirement if its primary purpose for FISA surveillance is to get evidence for a prosecution that is intended to advance a foreign intelligence purpose.[138] The analysis so far nonetheless lays part of the groundwork for analysis in Part III of: the lower federal courts' interpretation of the original FISA as imposing a "primary purpose" test; Congress's amendment of the original FISA's purpose provision; and the FISA courts' interpretation of the original FISA and the FISA as amended by the Patriot Act.

b. Minimization Procedures

The application for a FISA surveillance order must propose minimization procedures.[139] The judge reviewing the application must ensure that those proposed minimization procedures satisfy the statutory definition of minimization procedures.[140] Finally, the judge's order granting an application must "direct . . . that the minimization procedures be followed."[141] These provisions play an important role in the issue of whether the government can use FISA surveillance for prosecutorial purposes. They were the basis for the FISA Trial Court's conclusion in In re *Sealed Case* that the government cannot use FISA surveillance for the primary purpose of building a prosecution.[142]

The FISA defines "minimization procedures" to mean:

(1) specific procedures, which shall be adopted by the Attorney

---

[138] *See infra* notes 492–516 & 559–61 and accompanying text.

[139] *See* 50 U.S.C. § 1804(a)(5).

[140] *See id.* § 1805(a)(4).

[141] *Id.* § 1805(c)(2).

[142] FISA Trial Court Opinion, 218 F. Supp. 2d 611, 616–25 (Foreign Int. Surv. Ct. Rev. 2002); *see infra* notes 335–340 and accompanying text.

> General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
>
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e) (1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
>
> (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.[143]

The first two parts of the definition of "minimization procedures" aim to protect the privacy interests of U.S. persons. The third part aims to protect the government's interest in law enforcement. The fourth part of the definition has a fairly narrow application and is (at best modestly) relevant here only as further evidence of the FISA's solicitude for the privacy of U.S. persons.[144] We will therefore focus on the first three parts of the definition, the first two of which prescribes procedures protective of individual privacy, the third of which prescribes minimization procedures protective of law enforcement interests.

---

[143] 50 U.S.C. § 1801(h).

[144] The fourth part of the definition of minimization procedures, 50 U.S.C. § 1801(h)(4), addresses information acquired in FISA surveillance authorized under § 1802(a). Section 1802(a) empowers the Attorney General to authorize electronic surveillance without a court order if "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party" and other conditions are met. 50 U.S.C. § 1802(a)(1)(B).

The first part of the definition prescribes the general standard and requirements for the processes of acquiring, retaining, and disseminating nonpublicly available information about unconsenting U.S. persons ("U.S. person information").[145] That standard requires procedures that minimize the acquisition and retention—and prohibit the dissemination—of U.S. person information only to the extent that this minimization and prohibition can be "consistent with the need . . . to obtain, produce, and disseminate foreign intelligence information."[146] The procedures must only "minimize" acquisition and retention, whereas they must "prohibit" dissemination.[147] This reflects that sometimes the government must acquire and temporarily retain information to evaluate its usefulness but in that case the government should ultimately destroy, rather than disseminate, the information if it turns out to be extraneous.[148] The "consistent with" standard differs from one that would require the government to minimize the acquisition and retention, or prohibit the dissemination, of *all* information that is not "foreign intelligence information." It might be "consistent with" the government's need to obtain, produce, and disseminate information for the government at least temporarily to collect, retain, and disseminate U.S. person information on a limited basis, even though that information is not "necessary to" one of the five foreign intelligence purposes identified in the FISA's definition of "foreign intelligence information."[149]

---

[145] 50 U.S.C. § 1801(h)(1); *see* FISA Trial Court Opinion, 218 F. Supp. 2d at 623–25 (treating first portion of definition of "minimization procedures" as prescribing general standard); Banks, *supra* note 30, at 1177 (describing first portion of definition of "minimization procedures" as "generic").

[146] 50 U.S.C. § 1801(h)(1).

[147] *See* H.R. CONF. REP. NO. 95-1720, at 23 (1978) (modifying version of bill passed by House to differentiate between acquisition and retention, on the one hand, and dissemination, on the other hand, reflecting conference committee's judgment that "the standard for dissemination should be higher than for acquisition and retention").

[148] *See, e.g.*, S. REP. NO. 95-701, at 39 (1978) ("It is . . . obvious that no electronic surveillance can be so conducted that innocent conversations can be totally eliminated") (internal quotation marks and footnote omitted); H.R. REP. NO. 95-1283, pt. 1, at 56 (stating that extraneous information gathered by electronic surveillance "might be retained for a reasonable period in order to determine whether it did indeed relate to one of the approved purposes" for retaining information in longer term).

[149] *See* H.R. REP. NO. 95-1283, pt. 1, at 58:

> [T]he definition of "minimization procedures" does not state that only 'foreign intelligence information' can be acquired, retained, or disseminated. The committee recognizes full well that bits and pieces of information, which taken separately could not possibly be considered "necessary," may together or over time take on significance and become "necessary." Nothing in this definition is intended to forbid the retention or even limited dissemination of such bits and pieces before their full significance becomes apparent.

Id.; *see also id.* at 58–59 (explaining that government may need to retain information

One such situation is identified in the second part of the definition of "minimization procedures."[150] Sometimes information that identifies a U.S. person and that is not itself foreign intelligence information must be disseminated to enable the government to understand or assess the importance of other information that is foreign intelligence information. This identifying information "is not foreign intelligence information";[151] i.e., it is not "necessary to" any of the five foreign intelligence purposes identified in the definition of "foreign intelligence information."[152] Though not meeting that "necessity" standard, its dissemination would be "consistent with" the government's need to "produce" and "disseminate"—i.e., to evaluate and distribute to appropriate officials—foreign intelligence information, if its dissemination is "necessary to" understanding or assessing the importance of that foreign intelligence information.[153] This identifying information occupies a middle ground: It does not meet the strict "necessity" standard for foreign intelligence information but it also is not entirely extraneous, because it facilitates the gathering and processing of foreign intelligence information.

Information that identifies a U.S. person is not the only type of non-foreign intelligence information that can facilitate the gathering and processing of foreign intelligence information and that can accordingly be acquired, retained, and disseminated "consistent[ly] with" the government's need to gather and process foreign intelligence information. Identifying information is nonetheless dealt with specially in two ways: It is the subject of a separate subsection in the definition of "minimization procedures," and that subsection

---

about known spy's contacts and acquaintances even though most of them may turn out to be innocent; others who appear innocent "may merely be very sophisticated and well-versed in their espionage tradecraft").

[150] *See* H.R. REP. NO. 95-1283, pt. 1, at 58 (citing situation fitting that described in § 1801(h)(2) as "[a]n example" of why § 1801(h)(1) uses the "consistent with" standard for minimization procedures, rather than requiring minimization of all non-foreign intelligence information).

[151] 50 U.S.C. § 1801(h)(2).

[152] *See* 50 U.S.C. § 1801(e); *see also supra* notes 136–37 and accompanying text (explaining that definition of "foreign intelligence information" identifies five foreign intelligence purposes to which information must, if it concerns U.S. persons, necessarily relate).

[153] *See Senate Intelligence Hearing on FISA*, *supra* note 42, at 207 (describing committee amendment to provision defining "minimization procedures" and explaining that amendment authorizes dissemination of information that identifies a U.S. person when necessary to understand or assess importance of foreign intelligence information, rather than requiring information to meet "necessity" standards prescribed in definition of foreign intelligence information, because "it would be hard" for identifying information to meet latter standards, even though "it is useful information that would be entirely proper to disseminate").

prescribes an especially high standard for its dissemination (i.e., it must be "necessary" to understanding or evaluating the importance of foreign intelligence information).[154] This special treatment reflects that being associated with a foreign intelligence investigation is like being indicted: it can ruin one's life.[155] The FISA recognized that information identifying U.S. persons, as well as other types of non-foreign intelligence information, could be vital to processing foreign intelligence information—even though not itself foreign intelligence information—but wanted the dissemination of identifying information to be dealt with by specific procedures.[156]

Unlike the first and second parts of the FISA's definition of "minimization procedures," the third part does not use the term "foreign intelligence information."[157] Instead, it addresses "information that is evidence of a crime."[158] Obviously, a piece of information can be "evidence of a crime" without being either (1) "foreign intelligence information," or (2) information that must be temporarily retained for the purpose of analyzing whether that information or other information is foreign intelligence information.[159] Thus, by authorizing information that is "evidence of crime" to be "retained or disseminated for law enforcement purposes," the third part allows the retention and dissemination of information whether or not it is foreign intelligence information or facilitates the gathering and processing of foreign intelligence information.

This discussion of the FISA definition of minimization procedures ends by emphasizing two things about that definition. First, it reflects that electronic surveillance for foreign intelligence information cannot identify that information perfectly and instantaneously. Inevitably the surveillance will include non-foreign intelligence information. Thus, the definition does not demand the impossible; it does not forbid the collection of non-foreign intelligence information. Instead, it limits the use of such information. Second, the provisions reflect that

---

[154] *See* H.R. REP. NO. 95-1283, pt. 1, at 61 (describing § 1801(h)(2) as setting "special dissemination standard").

[155] *See Senate Intelligence Hearing on FISA*, *supra* note 42, at 115 (prepared statement of John Shattuck and Jerry Berman, ACLU) (quoting testimony of Sen. Mondale on S. 3197, 94th Cong. (1976), in which Mondale said, "[T]he fact is that if you get the right of Government to investigate Americans for things that are not crimes, there are ways of destroying persons without ever appearing in the court room.").

[156] *See* H.R. REP. NO. 95-1283, pt. 1, at 61–62.

[157] 50 U.S.C. § 1801(h)(3), *reproduced supra* in text accompanying note 143.

[158] *Id.*

[159] *See id.* § 1801(h)(1).

surveillance for foreign intelligence can produce evidence of crime.

c. Section 1806 of the FISA

Section 1806 of the FISA addresses the "Use of information" obtained under a FISA surveillance order.[160] Two portions of Section 1806 deserve our attention: the first sentence of Section 1806(a) and portions of Section 1806(b).

i. Section 1806(a)

The first sentence of Section 1806(a) makes the minimization procedures operate. It says:

> Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter.[161]

The definition of "minimization procedures," which was discussed above, is just a definition. The definition becomes a statutory mandate because of its incorporation into Section 1806(a). The FISA judge can ensure compliance with this mandate "[a]t or before the end of the period of time for which electronic surveillance is approved by an order or an extension."[162]

ii. Section 1806(b)

The definition of "minimization procedures," as made operative by the first sentence of § 1806(a), authorizes information acquired under the FISA "that is evidence of a crime" to be "retained or disseminated for law enforcement purposes."[163] The use of FISA-acquired information for "law enforcement purposes" is further addressed in Section 1806(b), which states:

> No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.[164]

---

[160] *Id.* § 1806.
[161] *Id.* § 1806(a).
[162] *Id.* § 1805(e)(3).
[163] *Id.* § 1801(h)(3).
[164] *Id.* § 1806(b).

Section 1806(b) thus puts a condition on the "disclos[ure]" of FISA-acquired information "for law enforcement purposes."[165] The information can be disclosed "for law enforcement purposes" only if disclosure is accompanied by the prescribed statement. In addition to requiring the prescribed statement, Section 1806(b) creates a further requirement: FISA-acquired information can be used "in a criminal proceeding" only with the Attorney General's approval.[166] These requirements ensure that prosecutors get Attorney General approval before using FISA acquired information in a criminal proceeding.[167] The purpose of requiring Attorney General approval seems to be to ensure that the use of FISA-acquired information for law enforcement purposes can be balanced against any intelligence concerns that might weigh against such use.[168]

The need for advance Attorney General approval at two separate stages—(1) before submission of the application for a FISA surveillance order; and (2) before information obtained under the order is used in a criminal proceeding—suggests that Congress did not contemplate evidence obtained under an order being used in criminal proceedings routinely. That suggestion relates to, though it does not resolve, the issue whether the government can obtain a FISA surveillance order for prosecutorial purposes.[169]

C. The "Primary Purpose" Test

Now we turn to a development in the case law that occurred as Congress was attempting to enact legislation regulating the government's use of electronic surveillance for foreign intelligence information.[170] Specifically, this section describes the origin and

---

[165] *Id.*

[166] *Id.*

[167] *See, e.g.*, S. REP. NO. 95-701, at 61 (1978) ("This provision is designed to eliminate circumstances in which a local prosecutor has no knowledge that evidence was obtained through foreign intelligence electronic surveillance.").

[168] *See* S. REP. NO. 95-604, at 54 (1977) ("For example, the Department of Justice may decline to prosecute rather than disclose the names of important witnesses and key informants."); S. REP. NO. 95-701, at 61 (1978) (same). An early version of the bill that became the FISA said that FISA-acquired information could be used for law enforcement of criminal law only if such use "outweigh[ed] the possible harm to the national security." S. 1566, 95th Cong. § 2526(a) (1977), *reprinted in Senate Intelligence Hearing on FISA*, *supra* note 42, at 151. That requirement was removed in conference, in the belief that "even without a statutory requirement, there will be an appropriate weighing of criminal law enforcement needs against possible harm to the national security." H.R. CONF. REP. NO. 95-1720, at 30 (1978).

[169] *See infra* notes 550–552 and accompanying text (discussing relevance of Attorney General approval requirement to validity of "primary purpose" test).

[170] As explained *supra* note 73, bills to regulate the executive branch's use of electronic

extension of the judicially developed "primary purpose" test. The test originated as a Fourth Amendment restriction on the executive branch's use of warrantless electronic surveillance. Several lower federal courts nonetheless adopted the primary purpose test as a restriction that FISA imposes on surveillance conducted with prior judicial approval.

1. Origin of the Primary Purpose Test

Before FISA was enacted in 1978, the government conducted electronic surveillance for foreign intelligence without warrants or any other type of prior judicial approval.[171] In 1967, the U.S. Supreme Court held that electronic surveillance by the government can be a "search" subject to the Fourth Amendment.[172] Between 1967 and 1978—the pre-FISA period during which electronic surveillance was subject to Fourth Amendment review—several lower federal courts addressed Fourth Amendment challenges to warrantless electronic surveillance for foreign intelligence. In *Zweibon v. Mitchell*, as discussed above, the D.C. Circuit suggested that in the absence of exigent circumstances all warrantless electronic surveillance—even for foreign intelligence information—is unconstitutional.[173] Three other courts of appeals, however, upheld warrantless electronic surveillance conducted for the sole or primary purpose of obtaining foreign intelligence information.

The earliest such case involved civil rights activist H. Rap Brown.[174] Brown challenged his conviction of a federal firearm offense on the ground that it was based on warrantless—and hence unconstitutional—wiretaps.[175] In *United States v. Brown*, the Third Circuit held that the warrantless wiretaps were constitutional because they were authorized by the President's delegate, the Attorney

---

surveillance for foreign intelligence were introduced in each year between 1973 and 1978, when FISA was finally enacted.

[171] *See supra* notes 37–71 and accompanying text (discussing history of warrantless electronic surveillance in the name of national security).

[172] *See* Katz v. United States, 389 U.S. 347, 353 (1967); *see also id.* at 359 n.23 ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."); *Berger*, 388 U.S. at 50–53 (holding that Fourth Amendment applied to state statute authorizing wiretaps for law enforcement purposes).

[173] Zweibon v. Mitchell, 516 F.2d 595 (1975), *discussed supra* notes 50–57 and accompanying text.

[174] United States v. Brown, 484 F.2d 418, 420–21 (1973), *cert. denied*, 415 U.S. 960 (1974). For a brief biography of H. Rap Brown, who changed his name to Jamil Abdullah Al-Amin, see http://www.spartacus.schoolnet.co.uk/USArapB.htm.

[175] *Brown*, 484 F.2d at 425.

General, "for the purpose of gathering foreign intelligence."[176] The court reasoned that "[r]estrictions upon the President's power which are appropriate in cases of domestic security become artificial in the context of the international sphere."[177] In a concurring opinion, Judge Goldberg emphasized that the wiretaps were for foreign intelligence, and not for other purposes such as building a prosecution or stifling political dissent: "This case in no way involved the spurious use of national security as a cover for warrantless electronic surveillance of accused and potential criminal defendants, domestic radicals, or political dissenters; and the panel opinion narrowly barricades warrantless wiretaps within the confines of legitimate foreign intelligence surveillance.[178] *Brown* is a leading case partly because the majority opinion was written by Judge Griffin Bell.[179] Judge Bell became Attorney General of the United States under President Jimmy Carter. In that position he led the Carter Administration's support for the original FISA.[180]

The next leading case also came from the Third Circuit, this time sitting en banc, in *United States v. Butenko*.[181] The defendants appealed convictions for their plan to steal military secrets for the Union of Soviet Socialist Republics.[182] They contended that the prosecutor violated the Fourth Amendment by using evidence from warrantless wiretaps.[183] The Third Circuit rejected that contention and held that the Fourth Amendment did not require prior judicial approval for the wiretaps in that case.[184] The court recognized that, generally, prior judicial approval "might have some salutary effects."[185] The court explained: "[A] judge, for example, could assure that the Executive was not using the cloak of foreign intelligence information gathering to engage in indiscriminate surveillance of domestic political organizations."[186] The government

---

[176] *Id.* at 426.

[177] *Id.*

[178] *Id.* (Goldberg, J., concurring).

[179] *Id.*

[180] *See, e.g.*, 124 CONG. REC. 10,887 (1978) (statement of Sen. Kennedy) ("Both Attorney General Bell and Attorney General Levi have been most cooperative and helpful in the drafting of the bill [S. 1566, 95th Cong. (1977)].").

[181] 494 F.2d 593 (Cir. 1974) (en banc), *cert. denied*, 419 U.S. 881 (1974).

[182] *See Butenko*, 494 F.2d at 616–17 (Aldisert, J., concurring in part and dissenting in part); *see also id.* at 596 n.1 (referring the reader to Judge Aldisert's opinion "for a fuller exposition of the factual background").

[183] *See id. at* 617–18 (Aldisert, J., concurring in part and dissenting in part).

[184] *See id.* at 602–06.

[185] *Id.* at 605.

[186] *Id.*

did not need prior judicial approval in the case before the court, however, "since the district court found that the surveillances . . . were 'conducted and maintained solely for the purpose of gathering foreign intelligence information.'"[187] Thus, the court in *Butenko*, like Judge Goldberg concurring in *Brown*, worried that the government could target electronic surveillance at "political" organizations but upheld the surveillance, despite the absence of a warrant, because it was for the purpose of obtaining foreign intelligence information. The court further held that, because the surveillance's "primary purpose" was to gather foreign intelligence information, it was reasonable within the meaning of the Fourth Amendment.[188] In so holding, the *Butenko* court distinguished the purpose of gathering foreign intelligence information, on the one hand, from the purpose of "looking for evidence of criminal conduct unrelated to the foreign affairs needs of a President."[189]

Although the Third Circuit in *Butenko* used a "primary purpose" test, the test is more often associated with the Fourth Circuit's later decision in *United States v. Truong Dinh Hung*.[190] *Truong*, like *Brown* and *Butenko*, involved warrantless electronic surveillance that occurred before the FISA took effect.[191] The Fourth Circuit did not issue its decision in *Truong*, however, until 1980, after the FISA took effect.[192] The legislative history accordingly does not cite the Fourth

---

[187] *Id.* (quoting *United States v. Butenko*, 318 F. Supp. 66, 72 (D.N.J. 1970)).

[188] *See id.* at 605–06.

[189] *Id.* at 606.

[190] 629 F.2d 908 (4th Cir. 1980); *see, e.g.*, *In re* Sealed Case, 310 F.3d at 725 (citing *Truong* as "the origin" of what government argued was false dichotomy between law enforcement and foreign intelligence underlying "primary purpose" test); U.S. Gen. Accounting Office, Report No. 01-780, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED, 13 n.16, 36 (July 2001) (citing only *Truong* as source of primary purpose test). In addition to *Butenko*'s use of a "primary purpose" test before *Truong*, Judge Wilkey endorsed a primary purpose test in *Zweibon*, which pre-dated *Truong*, for the purpose of determining whether electronic surveillance was subject to Title III's requirements. *See Zweibon v. Mitchell*, 516 F.2d 594, 69 (D.C. Cir. 1975) (Wilkey, J., concurring in part and dissenting in part):

> The function which the surveillance [before the court] was intended to serve was not primarily one of uncovering evidence of domestic crime. . . . It was an intelligence operation undertaken pursuant to the President's constitutional power to conduct this country's foreign affairs, as distinct from his duty to administer domestic criminal legislation.

Id.

[191] FISA § 301 ("Effective date of Act Oct. 25, 1978"); *Truong*, 629 F.2d at 912 (stating that electronic surveillance of Truong occurred from May 1977 to Jan. 1978).

[192] *See Truong*, 629 F.2d at 908.

Circuit's decision in *Truong*.[193] *Truong* remains important, however, for two reasons. First, it was the first appellate case ever to suppress evidence under the primary purpose test. Second, it furnished a springboard for lower courts: In cases after *Truong* involving surveillance under FISA surveillance orders, lower courts would cite *Truong* and rely on its reasoning to apply the "primary purpose" test, which had been developed for pre-FISA, warrantless electronic surveillance, to surveillance authorized under judicially issued FISA surveillance orders.[194]

In *Truong*, the FBI tapped the phone and bugged the apartment of Mr. Truong for evidence that he was sending classified information to the government of Vietnam.[195] The FBI did not have a warrant or any other judicial authorization for electronic surveillance of Truong.[196] The government used evidence gathered through the surveillance to convict Truong of espionage and other crimes.[197] Truong challenged his convictions contending that the warrantless electronic surveillance violated the Fourth Amendment.[198]

The Fourth Circuit, upholding this challenge in part, held that the surveillance violated the Fourth Amendment starting on July 20, 1977.[199] On that day, judging from internal Justice Department memoranda, the investigation "became primarily a criminal investigation."[200] The court upheld the admission of evidence obtained before that date under a "foreign intelligence exception to the warrant requirement"[201] of the Fourth Amendment. In the court's

---

[193] *Cf.* 124 CONG. REC. 10,887 (1978) (statement of Sen. Kennedy) (referring to "prosecutions in the Humphrey and Truong cases" to "point out the need" for legislation such as FISA); H.R. REP. NO. 95-1283, pt. 1, at 109 (1978) (additional views of Reps. Morgan F. Murphy and Charles Rose) (referring to pending *"Truong/Humphrey* case"); *id.* at 112 n.6 (dissenting views on H.R. 7308) (citation to memorandum opinion of district court in same case).

[194] *See infra* notes 209–25 and accompanying text.

[195] *Truong*, 629 F.2d at 911–12.

[196] *Id.* at 912. It is unclear why the FBI did not obtain a warrant for the surveillance of Truong under Title III, which was then on the books and authorized electronic surveillance for evidence of espionage, the crime of which Truong was ultimately convicted. The Fourth Circuit simply noted: "The practical difficulties of obtaining a warrant for foreign intelligence surveillance were particularly acute at the time this surveillance was conducted, because Title III . . . , which specifies warrant procedures, contained no procedures tailored to foreign intelligence surveillance." *Id.* at 913 n.2.

[197] *Id.* at 912.

[198] *Id.*

[199] *Id.* at 916.

[200] *Id.* (describing memorandum as "indicating that the government had begun to assemble a criminal prosecution").

[201] *Id.*

view, however, the exception applies only when the executive "is attempting primarily to obtain foreign intelligence."[202] The exception does not apply "if the government is primarily attempting to put together a criminal prosecution,"[203] as occurred starting on July 20, 1977, in the case before it. The court of appeals said the Fourth Amendment puts this "primary purpose" limit on the foreign intelligence exception to the warrant requirement because, "once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution."[204] Since the surveillance of Truong predated the FISA, the court did not address whether the FISA fell short, satisfied, or went beyond "the constitutional minimum described in [its] opinion."[205]

Truong's "primary purpose" test was more restrictive than *Butenko* in two ways. First, *Butenko* suggested that the government could not use warrantless electronic surveillance to get "evidence of criminal conduct unrelated to the foreign affairs needs of a President."[206] *Truong*, more restrictively, held that the government could not use warrantless electronic surveillance even to get evidence of a crime—namely espionage—that did relate to the foreign affairs needs of the President.[207] Second, *Truong* determined the "primary purpose" of the surveillance by evaluating contacts between the intelligence officials involved in the case and the prosecutors.[208] The link, however, between the "primary purpose" of surveillance and the degree of contact between intelligence officials and prosecutors is not inevitable. In these two respects, *Truong* deserves credit as the

---

[202] *Id.*

[203] *Id.*

[204] *Id.* at 915.

[205] *Id.* at 914 n.4:

> While the [FISA] suggests that it is possible for the executive branch to conduct at least some types of foreign intelligence surveillance while being subject to a warrant requirement, the complexity of the statute also suggests that the imposition of a warrant requirement, beyond the constitutional minimum described in this opinion, should be left to the intricate balancing performed in the course of legislative process by Congress and the President.

Id.

[206] United States v. Butenko, 494 F.2d 593, 606 (3d Cir. 1974).

[207] *Truong*, 629 F.2d at 908.

[208] *Id.* at 916.

progenitor of the "primary purpose" test that became associated with the FISA. As discussed below, that test, like the *Truong* opinion, assumes that the purpose of gathering foreign intelligence information is incompatible with the purpose of getting evidence for prosecution, even prosecutions for crimes involving foreign intelligence; and that, to satisfy the test, contacts between intelligence officials and prosecutors must be minimized.

2. Linkage of the "Primary Purpose" Test to the FISA

Truong held that warrantless electronic surveillance violated the Fourth Amendment because the government was "primarily attempting to put together a criminal prosecution" rather than "to obtain foreign intelligence."[209] Although *Truong* used this "primary purpose" test as a Fourth Amendment restriction on warrantless surveillance, other lower courts later used the test to restrict surveillance conducted with prior judicial approval under the FISA.

An early case linking the primary purpose test to the FISA was *United States v. Megahey*.[210] In *Megahey*, a New York federal district court said that FISA surveillance was "appropriate only if foreign intelligence surveillance is the Government's primary purpose."[211] The court found that standard satisfied and upheld a conviction based partly on evidence obtained under a FISA surveillance order.[212] In affirming the conviction (in an opinion named for a different defendant), the Second Circuit in *United States v. Duggan*, agreeing with the district court in *Megahey*, found "plain" in the text of the FISA "[t]he requirement that foreign intelligence information be the primary objective of the surveillance."[213] The Second Circuit also agreed with the district court that the FISA surveillance in that case "was to secure foreign intelligence information and was not . . . directed towards criminal investigation or . . . criminal prosecution.'"[214]

Duggan is important for three reasons. First, it adopted the primary purpose test as a restriction imposed by the FISA. The Fourth

---

[209] *Id.*

[210] 553 F. Supp. 1180 (E.D.N.Y. 1982), *aff'd sub nom.* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

[211] *Megahey*, 553 F. Supp. at 1189–90.

[212] *See id.* at 1189–90.

[213] *Duggan*, 743 F.2d at 77.

[214] *Id.* at 78 (internal quotations marks omitted) (quoting *Megahey*, 553 F. Supp. at 1190).

Amendment influenced the court's interpretation of the FISA, but its holding rested on statutory interpretation.[215] Second, the *Duggan* court described the test as distinguishing between the purpose of gathering foreign intelligence and the purpose of gathering evidence for a prosecution.[216] That description does not contemplate that the government's purposes could be to gather information that is both foreign intelligence information and evidence of crime—e.g., a plan by international terrorists to bomb a U.S. government building—and to use that information for a prosecution that serves foreign intelligence objectives by, for example, preventing conduct that both violates federal criminal law and harms national security. Third, *Duggan* traced the primary purpose test to the purpose provision of the original FISA—i.e., the provision that required a certification that "the purpose of the surveillance is to obtain foreign intelligence information."[217]

All three aspects of *Duggan* gained acceptance in other courts. The First Circuit's decision in *United States v. Johnson* supplies a good example.[218] The *Johnson* court upheld the defendants' convictions for U.S.-based terrorist acts against the British in Northern Ireland.[219] To

---

[215] *See id.* at 77 ("The requirement that foreign intelligence information be the primary objective of the surveillance is plain not only from the language of [FISA] § 1802(b) but also from the requirements in § 1804 as to what the application must contain."); *see also id.* (articulating primary purpose test in addressing defendants' "conten[tion] that the surveillance . . . was not authorized by FISA because the information was sought as part of a criminal investigation").

[216] *Id.* at 78 (noting that FISA surveillance in that case was "to secure foreign intelligence information and was not . . . directed towards criminal investigation or . . . criminal prosecution") (quoting *Megahey*, 553 F. Supp. at 1190).

[217] *See id.* at 77 (citing 50 U.S.C. § 1804(a)(7) (Supp. V. 1981) (amended 2001)). In addition to relying on the "purpose" provision in the original FISA, the court in *Duggan* also relied on the FISA provision that requires a government official to explain the basis for his or her belief that the information sought is the type of foreign intelligence information described in the application, *see* 50 U.S.C. § 1804(a)(7)(E)(i) (2000) (amended 2001), and FISA § 1802(b), which refers to a court's authority to "approv[e] electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information," 50 U.S.C. § 1802(b) (2000) (amended 2001). *See Duggan*, 743 F.2d at 77.

[218] 952 F.2d 565 (1st Cir. 1991); *accord* United States v. Badia, 827 F.2d 1458, 1462, 1464 (11th Cir. 1987) (finding, contrary to defendant's contention, that FISA surveillance "did not have as its purpose the primary objective of investigating a criminal act. Rather, surveillance was sought for the valid purpose of acquiring foreign intelligence information"); United States v. Pelton, 835 F.2d 1067, 1074–76 (4th Cir. 1987) (rejecting defendant's contention that FISA surveillance of him "was not conducted for 'foreign intelligence purposes' as required by the statute"; agreeing with district court that "the 'primary purpose of the surveillance, both initially and throughout, was to gather foreign intelligence information"); *cf.* United States v. Bin Laden, 126 F. Supp. 2d 264, 277–78 (S.D.N.Y. 2000) (adopting primary purpose test to assess Fourth Amendment challenge to warrantless surveillance for foreign intelligence overseas).

[219] *See Johnson*, 952 F.2d at 569.

get those convictions, the government used evidence obtained under FISA surveillance orders.[220] On appeal, the defendants challenged the FISA surveillance "on the ground that it was undertaken not for foreign intelligence purposes, but to gather evidence for a criminal prosecution."[221] The court, applying the primary purpose test, rejected the challenge. After referring to the purpose provision of the FISA, the court said that, "[a]lthough evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance."[222] To support that statement, the Johnson court cited *Duggan* and *Truong*.[223]

Some courts that have adopted the primary purpose test as a FISA-imposed restriction have done so even though they recognized that information gathered through FISA surveillance sometimes would be used for prosecution, and that Congress approved such use in FISA's text and legislative history.[224] These courts apparently trusted their ability to determine when prosecutorial use was the government's primary purpose for the FISA surveillance; *Truong* indicated this determination could be based on contacts between intelligence officials and prosecutors. Despite that guidance and *Truong*'s suppression of evidence, no court ever used *Truong*'s primary purpose test to suppress evidence acquired under the FISA.[225] Perhaps that is because the Department of Justice, which prepares and

---

[220] *See id.* at 571.

[221] *Id.* at 572.

[222] *Id.*

[223] *Id. But cf.* United States v. Sarkissian, 841 F.2d 959, 964–65 (9th Cir. 1988) (declining to decide whether FISA surveillance had to satisfy "primary purpose" test and "refus[ing] to draw too fine a distinction between criminal and intelligence investigations"); United States v. Falvey, 540 F. Supp. 1306, 1313–14 (E.D.N.Y 1982) (rejecting defendants' argument that FISA surveillance was invalid because "the Government was clearly conducting a routine criminal investigation" and distinguishing *Truong* as involving warrantless search, inapplicable to FISA searches because FISA prescribes a warrant procedure).

[224] *See, e.g., Johnson*, 952 F.2d at 572 ("[E]vidence obtained under FISA subsequently may be used in criminal prosecutions."); *Duggan*, 743 F.2d at 78 ("[W]e emphasize that otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of such surveillance may later be used, as allowed by § 1806(b), as evidence in a criminal trial. Congress recognized that in many cases the concerns of the government with respect to foreign intelligence will overlap those with respect to law enforcement.").

[225] *See In re* Sealed Case, 310 F.3d 717, 727 (Foreign Int. Surv. Ct. Rev. 2002) (observing that court of appeals decisions adopting the primary purpose test as a gloss on the FISA "affirm district court opinions permitting the introduction of evidence gathered under a FISA order").

submits all applications for FISA surveillance,[226] implemented the test so vigorously, as discussed next.

D. The Department of Justice's Use of the Primary Purpose Test as the Foundation for the Wall

The Department of Justice implemented the primary purpose test by building a high wall between foreign intelligence officials and law enforcement officials. More specifically, what the public came to know as "the wall" arose from (1) the case law discussed above adopting the "primary purpose" test as an interpretation of the original FISA's "purpose" provision; (2) internal procedures adopted by the Department to implement the primary purpose test; and (3) the interpretation of those procedures by Department officials and the FISA Trial Court.[227] This section discusses the latter two developments, relying mostly on government reports, including the final report of the 9/11 Commission.[228]

Until the early 1990s the Department used informal procedures to ensure that FISA surveillance did not take on the "primary purpose" of gathering evidence for prosecution.[229] The Department's prosecutors obtained foreign intelligence information gathered through the FISA process with "the understanding . . . that they would not improperly exploit that process for their criminal cases."[230] The prosecutors' main source of foreign intelligence information was the FBI, which conducts almost all FISA surveillance targeting U.S. persons for counterintelligence.[231] "Whether the FBI shared with

---

[226] *See* Exec. Order No. 12,333, pt. 2.5, 3 C.F.R. (1981), *reprinted in* 50 U.S.C. § 401 (2000) (delegating to Attorney General power to authorize FISA surveillance).

[227] *See infra* notes 243–62 and accompanying text.

[228] *See generally* 9/11 COMM'N REPORT, *supra* note 2, at 78–80 (section entitled "Legal Constraints on the FBI and 'The Wall'"); REPORT OF THE JOINT INQUIRY, *supra* note 13, at xvii, 80–84 (pagination from unclassified version of report) (discussing role of "the wall" in events leading up to 9/11); U.S. General Accounting Office, Report No. 01-780, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED, (July 2001); U.S. Department of Justice, FINAL REPORT OF THE ATTORNEY GENERAL'S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NATIONAL LABORATORY INVESTIGATION, 707–62 (May 2000) (Chapter 20 entitled "'Primary Purpose' and the Sharing of Intelligence Information Among the FBI, OIPR, and the Criminal Division") [hereinafter "BELLOWS REPORT" after the name of the lawyer who headed the team]; Office of the Inspector General, U.S. Department of Justice, *The Handling of FBI Intelligence Information Related to the Justice Department's Campaign Finance Investigation, Unclassified Executive Summary*, § 5.A.2 (July 1999) (addressing problems of intelligence sharing within Department of Justice); Hill, *Joint Inquiry Staff Statement*, *supra* note 3, at 21–26 (section entitled "The Wall").

[229] *See* 9/11 COMM'N REPORT, *supra* note 2, at 78.

[230] *Id.*

[231] *See* Exec. Order No. 12,333, § 1.14(a), 3 C.F.R. 200,212 (1981), *reprinted in* 50

prosecutors information pertinent to possible criminal investigations was left solely to the judgment of the FBI."[232] This informal arrangement apparently worked because of the knowledge and experience of Mary Lawton, the head of the Justice Department's Office of Intelligence Policy and Review (OIPR) until 1993.[233] OIPR was and remains the office that prepares applications for FISA surveillance and presents them to the FISA Trial Court for approval.[234]

By the 1990s the Department of Justice had gotten "sloppy" about complying with the primary purpose test, according to Lawton's successor, Richard Scruggs.[235] Scruggs went to Attorney General Janet Reno about it.[236] Scruggs told Reno that, in particular, he worried about contacts between the FBI and Justice Department prosecutors in the Aldrich Ames investigation, which included FISA surveillance.[237] Indeed, Scruggs told Reno he worried that these contacts violated the FISA and caused some of Reno's certifications in the FISA applications to be inaccurate.[238] Reno became "very upset" and told Scruggs to "make sure this did not happen again."[239] After Ames pleaded guilty to espionage in 1994, FBI headquarters made clear that FBI agents should not contact Criminal Division

---

U.S.C. § 401 note (providing that the Director of FBI "shall . . . within the United States conduct counterintelligence and coordinate counterintelligence activities of other agencies within the Intelligence Community" and shall "[p]roduce and disseminate foreign intelligence and counterintelligence"); Exec. Order 12,036, § 1-1401 (similar provision in predecessor order in effect when FISA was enacted), 43 Fed. Reg. 3674 (1978); *see also Senate Intelligence Hearing on FISA*, *supra* note 42, at 15 (statement of Attorney General Griffin Bell) (stating that most electronic surveillance under bill that became the FISA would be conducted by either the FBI or the National Security Agency); 9/11 COMM'N REPORT, *supra* note 2, at 423 (observing that in the 1980s and 1990s FBI "was the lead agency for the investigation of foreign terrorist groups operating in the United States").

[232] 9/11 COMM'N REPORT, *supra* note 2, at 78.

[233] *See* BELLOWS REPORT, *supra* note 228, at 712 (stating that informal system "appears to have worked quite satisfactorily while Mary Lawton was the head of OIPR, both from the perspective of the Criminal Division and from that of the FBI").

[234] *See* 28 C.F.R. § 0.33b (2004); *see also* United States Attorneys' Manual, § 1-2.106 (stating that OIPR "prepares certifications and applications" for FISA surveillance).

[235] BELLOWS REPORT, *supra* note 228, at 712.

[236] *Id.* at 712–13.

[237] *See* 9/11 COMM'N REPORT, *supra* note 2, at 78 ("[T]he prosecution of Aldrich Ames for espionage in 1994 revived concerns about the prosecutors' role in intelligence investigations"; Richard Scruggs "complained to Attorney General Janet Reno about the lack of information-sharing controls."); BELLOWS REPORT, *supra* note 228, at 713 (to the same effect); *see also* 9/11 COMM'N REPORT, *supra* note 2, at 91 (explaining that Ames was CIA officer who, "[t]hough obviously unreliable, had been protected and promoted by fellow officers while he paid his bills by selling to the Soviet Union the names of U.S. operatives and agents, a number of whom died as a result").

[238] BELLOWS REPORT, *supra* note 228, at 713.

[239] *Id.*

prosecutors without OIPR's approval; violation of this by an FBI agent would be a "career stopper."[240] Thereafter, OIPR "became the gatekeeper for the flow of FISA information to criminal prosecutors."[241] OIPR played this role with a vengeance, conveying to the FBI "the overarching message . . . that contact with the Criminal Division is dangerous, either because future FISA coverage will not be approved or because existing FISA coverage will be taken down."[242]

After much internal debate, in July 1995 the Attorney General adopted written procedures to implement the primary purpose test.[243] As interpreted by Justice Department officials, the July 1995 procedures erected "the wall."[244] Three particular provisions of the procedures did most of the wall-building work. The three provisions applied to all foreign intelligence (FI) or foreign counterintelligence (FCI) investigations in which the FBI conducted FISA surveillance.[245]

One provision prohibited the Criminal Division from giving the FBI advice that would "result in either the fact or the appearance of the Criminal Division's directing or controlling the FI or FCI

---

[240] *Id.* at 714; *see also* 9/11 COMM'N REPORT, *supra* note 2, at 79.

[241] 9/11 COMM'N REPORT, *supra* note 2, at 78.

[242] BELLOWS REPORT, *supra* note 228, at 731.

[243] Memorandum of from Janet Reno, Attorney General, U.S. Dep't of Justice, to Assistant Attorney General, Criminal Division, U.S. Dep't of Justice; Director, FBI, U.S. Dep't of Justice; Counsel for Intelligence Policy, U.S. Dep't of Justice; United States Attorneys, U.S. Dep't of Justice, "Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations," *available at* http://www.fas.org/irp/agency/doj/fisa/1995procs.html (July 19, 1995) [hereinafter 1995 Att'y Gen. Procedures]; *see also* BELLOWS REPORT, *supra* note 228, at 714–21 (describing development of 1995 guidelines); *id.* at 721 (quoting explanation of draft of 1995 procedures stating that restrictions were "[t]o avoid running afoul of the 'primary purpose' test").

[244] *See* 9/11 COMM'N REPORT, *supra* note 2, at 79 (stating that July 1995 procedures "were almost immediately misunderstood and misapplied . . . Over time the procedures came to be referred to as 'the wall.'"); REPORT OF THE JOINT INQUIRY, *supra* note 13, at 83 (pagination from unclassified version of report) (finding that many in FBI misunderstood Attorney General's 1995 procedures); U.S. General Accounting Office, REPORT NO. 01-780, *supra* note 228, at 4 (July 2001) ("[T]he implementation and interpretation of the [Attorney General's 1995 procedures] and the previously noted concerns led to a significant decline in coordination between the FBI and the Criminal Division.").

[245] The provisions were entitled procedures "for Contacts Between the FBI and the Criminal Division." 1995 Att'y Gen. Procedures, *supra* note 243, at 1. They also, however, regulated contacts between the FBI and the U.S. Attorneys Offices. *See id.* Generally, they required the FBI to contact U.S. Attorneys' Offices only with approval of the Criminal Division and OIPR. *See id.* at § A.2 ("The FBI shall not contact a U.S. Attorney's Office concerning [an FI or FCI investigation using FISA surveillance] without the approval of the Criminal Division and OIPR.").

investigation toward law enforcement objectives."[246] This provision had particular bite because it banned even "the appearance" of Criminal Division direction and control.[247] Although the provision allowed Criminal Division advice aimed at "preserving" the possibility of prosecution, it seemed by negative implication to bar advice aimed at "enhancing" the possibility of a prosecution.[248] In practice, the line between preserving and enhancing advice was so murky that advice-giving was substantially curtailed.[249] Moreover, the provision did not define "directing or controlling," which led to different interpretations.[250] Beyond that, it seemed to restrict the Criminal Division's participation in, not just the FISA surveillance, but all aspects of an investigation (including, e.g., physical surveillance).[251] Consequently, prosecutors in the Justice Department failed to receive important information from not only the FBI (which did the FISA surveillance) but also from other agencies involved in the non-FISA aspects of intelligence investigations, such as the National Security Agency and the CIA.[252]

---

[246] *Id.* at § A.6.

[247] *See* BELLOWS REPORT, *supra* note 228, at 719 (stating that "appearance" formulation, coupled with other wording in 1995 procedures, was "considerably . . . problematic"); *id.* at 729 (describing "appearance" formulation as one aspect of 1995 procedures that—more than preventing the Criminal Division from being "at the table" during FISA investigations—kept the Criminal Division out of "the neighborhood"); *id.* at 750 (citing "appearance" formulation as one aspect of 1995 procedures that, as implemented by OIPR, "crippled" the Criminal Division's ability to carry out "what ought to be one of its core functions").

[248] *See* 1995 Att'y Gen. Procedures, *supra* note 243, at § A.6.

[249] *See* BELLOWS REPORT, *supra* note 228, at 721–34.

[250] *See id.* at 727–30.

[251] *See* 9/11 COMM'N REPORT, *supra* note 2, at 79 (1995 procedures were interpreted to restrict information sharing and coordination even in investigations where FISA surveillance had not been used); BELLOWS REPORT, *supra* note 228, at 719, 729, 750 (citing investigation-wide scope of proposed 1995 procedures as one aspect that was "considerably . . . problematic"); *id.* at 729 (citing investigation-wide aspect of 1995 procedures as one aspect of 1995 procedures that—more than preventing the Criminal Division from being "at the table" during FISA investigations—kept the Criminal Division out of "the neighborhood"); *id.* at 750 (citing investigation-wide scope of 1995 procedures as one aspect of them that, as applied by OIPR, "crippled" the Criminal Division's ability to carry out "what ought to be one of its core functions").

[252] 9/11 COMM'N REPORT, *supra* note 2, at 79. The Church Committee reports indicate that the NSA and CIA, as well as FBI intelligence officials, withheld intelligence information from Justice Department prosecutors even before the Department of Justice adopted formal procedures walling-off prosecutors from intelligence officials. *See, e.g.*, *Church Committee Final Report*, *supra* note 64, at 39, 59, 86, 103 n.473, 130, 149–52, 273–74, 284. Professor Funk suggests that this was partly because of concern about the legality of sharing intelligence information with prosecutors and partly because of concern that the use of intelligence for prosecutions would compromise intelligence sources and methods. E-Mail from William F. Funk, Professor of Law, Lewis & Clark Law School, to Richard H. Seamon (Oct. 2, 2004).

Another provision of the 1995 procedures required the FBI and OIPR to notify the Criminal Division whenever an investigation using FISA surveillance developed evidence "that reasonably indicate[s] that a significant federal crime has been, is being, or may be committed."[253] This provision did not explain the term "significant" or the timing or procedures for the FBI and OIPR to notify the Criminal Division. Without guidance, the FBI and OIPR violated the notification requirement, sometimes by not notifying the Criminal Division at all and, other times, by delaying notification until it was too late for Criminal Division input to do any good.[254]

Finally, the 1995 procedures were interpreted to make the OIPR a gatekeeper that controlled (1) the flow of foreign intelligence information that could go from the FBI to the Criminal Division as well as (2) the flow of advice about potential prosecutions that could go from the Criminal Division to the FBI.[255] This meant, among other things, that an OIPR lawyer attended any meeting at which FBI agents and Criminal Division lawyers discussed intelligence investigations.[256] Because OIPR took such a stringent view of the separation required between the FBI and the Criminal Division under the 1995 Guidelines, those meetings were "not the ordinary interaction between agents and prosecutors"; rather, they were "surreal" and "weird."[257] In other ways, too, according to a later internal review, "OIPR has effectively crippled the Criminal Division's ability to carry out what ought to be one of its core functions, which is to provide advice and guidance at critical junctures during FCI investigations."[258]

OIPR was apparently acting under pressure from the FISA Trial Court. OIPR regularly told that court about "consultations and discussions between the FBI, the Criminal Division, and U.S. Attorney's offices in cases where there were overlapping intelligence and criminal investigations or interests."[259] Furthermore, sometimes the court itself acted as a self-described "'wall' so that FISA

---

[253] 1995 Att'y Gen. Procedures, *supra* note 243, at § A.1.

[254] BELLOWS REPORT, *supra* note 228, at 723–26.

[255] 9/11 COMM'N REPORT, *supra* note 2, at 78.

[256] *See* BELLOWS REPORT, *supra* note 228, at 733–34.

[257] *Id.* at 732; *see also id.* at 756 ("The practice of requiring prior notice to OIPR [of contacts between the FBI and the Criminal Division] . . . has served to stifle communications between the Criminal Division and the FBI.").

[258] *Id.* at 750.

[259] FISA Trial Court Opinion, 218 F. Supp. 2d 611, 620 (Foreign Int. Surv. Ct. Rev. 2002).

information could not be disseminated to criminal prosecutors without the Court's approval."[260] This happened "[i]n significant cases, involving major complex investigations such as the bombings of the U.S. Embassies in Africa, and the millennium investigations, where criminal investigations of FISA targets were being conducted concurrently, and prosecution was likely."[261] The result was that "[t]he wall in FISA matters became thicker and higher over time."[262]

Even before 9/11, the wall hurt the Justice Department's ability to protect national security from foreign threats. So concluded reports by the General Accounting Office (GAO) and the Justice Department. The GAO found that the wall hampered the Department's investigation into efforts by the People's Republic of China to influence U.S. political campaigns.[263] The Justice Department found that the wall also "adversely and materially affect[ed]" the investigation during the 1980s and 1990s of Wen Ho Lee, a nuclear scientist at the Los Alamos National Laboratory.[264] The GAO Report

---

[260] *Id.*

[261] *Id.*; *see also* 9/11 COMM'N REPORT, *supra* note 2, at 539 n.83 (noting that in 1990s FISA Trial Court "began designating itself as the gatekeeper for the sharing of intelligence information"). For a description of the embassy bombings to which the court was referring, *see id.* at 68–70 (section entitled "Embassy Bombings"). For background on the millennium investigation to which the court was referring, *see id.* at 174–82 (section entitled "The Millennium Crisis").

[262] *Hill, Joint Inquiry Staff Statement*, *supra* note 3, at 24. In addition to pressure from the FISA Court, the Justice Department got some pressure from congressional oversight committees, *see* THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978: THE FIRST FIVE YEARS, S. REP. NO. 98-660, at 15 (1984) (stating that "the Justice Department should" not use FISA "when it is clear that the main concern with respect to a terrorist group is domestic law enforcement and criminal prosecution"); IMPLEMENTATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, H.R. REP. NO. 98-738, at 6 (1984) (arguing that "the wiser course" is not to use FISA "once prosecution is contemplated, unless articulable reasons of national security dictate otherwise"); *see also* 50 U.S.C. § 1808(a)(1) ("On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning all electronic surveillance under this subchapter.").

[263] OFFICE OF THE INSPECTOR GENERAL, DEPT. OF JUSTICE, THE HANDLING OF FBI INTELLIGENCE INFORMATION RELATED TO THE JUSTICE DEPARTMENT'S CAMPAIGN FINANCE INVESTIGATION, UNCLASSIFIED EXECUTIVE SUMMARY, § 5.A.2 (1999) (recommending that "the Criminal Division, OIPR, and the FBI resolve the issue of their conflicting understandings of the Departmental guidelines concerning intelligence-sharing, and that the guidelines be amended accordingly"); *see also* GAO Report No. 01-780, *supra* note 228, at 1 (July 2001) (citing investigation of possible Chinese infiltration of U.S. political campaigns as one that "brought to light serious problems that have limited whether and when the FBI coordinates into investigations with the Department of Justice's (DOJ) Criminal Division"); *id.* at 3 (finding that "[a] key factor" in lack of coordination between Criminal Division and FBI was "concern over how the [courts] might rule on the primary purpose of the [FISA] surveillance or search in light of such coordination").

[264] BELLOWS REPORT, *supra* note 228, at 13; *see also* Draft Report of the Subcomm. on Dep't of Justice Oversight of Sen. Judiciary Comm., 147 CONG. REC. S13,803 (daily ed. Dec. 20, 2001).) (FISA surveillance of Wen Ho Lee was not sought because of concern

more generally concluded that a "key factor" in the intelligence-sharing problems in these investigations was the Department's efforts to satisfy the primary purpose test.[265]

It is the wall's apparent role in the 9/11 attacks, however, that seared it into national consciousness.[266] That apparent role came to light largely through an e-mail that was sent shortly before 9/11 and became public on about the first anniversary of the attacks. The e-mail was from a New York FBI agent who, because of the supposed wall, was not allowed to participate in a hunt for one of the men who, a few weeks later, would be a 9/11 hijacker:

> Whatever has happened to this—someday someone will die—and wall or not—the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.' Let's hope the [FBI's] National Security Law Unit will stand behind their decisions then, especially since the biggest threat to us now, UBL [Usama bin Laden], is getting the most "protection."[267]

This e-mail came to light in September 2002 during congressional hearings on the 9/11 attacks.[268] Those hearings produced a report finding that, in the summer before 9/11, the wall "led to a diminished level of coverage of suspected al-Qa'ida operatives in the United States."[269]

---

inside Justice Department that investigation had become "way too criminal").

[265] GAO Rep No. 01-780, *supra* note 228, at 3.

[266] *See* 9/11 COMM'N REPORT, *supra* note 2, at 269–72. Before 9/11, the Department changed the 1995 procedures twice—once after the internal inquiry report on the Wen Ho Lee investigation and again after the GAO report on the campaign finance. *See In re* Sealed Case, 310 F.3d at 728. General Reno approved the first set of changes on January 21, 2000. Under those changes, the FBI had to start (1) automatically sending the Criminal Division Letterhead Memoranda on certain foreign counterintelligence investigations (FCI) and (2) briefing the Division on FCI investigations once a month. *See* Memorandum for the Attorney General Through the Deputy Attorney General From Gary G. Grindler and Jonathan D. Schwartz, to Recommend that the Attorney General Authorize Certain Measures Regarding Intelligence Matters in Response to the Interim Recommendations Provided by Special Litigation Counsel Randy Bellows (approved by Attorney General Janet Reno on Jan 21, 2000), *available at* http://fas.org/irp/agency/doj/fisa/ag012100.html. The Deputy Attorney General made the second set of changes in August 2001, about one month before 9/11; they clarified some parts of the 1995 procedures and prescribed some new procedures designed to expand the information flow from the FBI to the Criminal Division. *See* Memorandum from Larry D. Thompson, Deputy Attorney General, on Intelligence Sharing, (Aug. 6, 2001), *available at* http://fas.org/irp/agency/doj/fisa/dag080606.html.

[267] 9/11 COMM'N REPORT, *supra* note 2, at 271; REPORT OF THE JOINT INQUIRY, *supra* note 13, at 84.

[268] REPORT OF THE JOINT INQUIRY, *supra* note 13, at 84; *see, e.g.*, Frank Davies, *Agent's pre-9/11 e-mail: 'Someday someone will die,'* MIAMI HERALD, Sept. 20, 2002, at A1.

[269] REPORT OF THE JOINT INQUIRY, *supra* note 13, at xvii.

The wall's role in the United States' failure to prevent the 9/11 attacks again drew national attention during proceedings of the "9/11 Commission."[270] Many witnesses testified that the wall hurt the government's ability to investigate and protect against terrorism before 9/11.[271] The Commission's staff found that "domestic counterterrorism efforts were impaired" by the wall.[272] Attorney General Ashcroft went farther. He testified before the 9/11

---

[270] The official name is the National Commission on Terrorist Attacks Upon the United States. The Commission was created by federal statute. *See* Intelligence Authorization Act for Fiscal Year 2003, Pub. L. No. 107-306, §§ 601–611, 116 Stat. 2408 (2002); *see also* Pub. L. No. 108-207, 118 Stat. 556 (2004) (extending life of commission).

[271] *See, e.g.*, Stewart A. Baker, Prepared Testimony for the 9/11 Comm'n, at 7–11 (Dec. 8, 2003) (explaining that "we missed our best chance" to prevent 9/11 attacks because of the wall); William P. Barr, Prepared Statement to 9/11 Comm'n at Sixth Public Hearing (Dec. 8, 2003) (unpaginated) ("Prohibitions on . . . using intelligence information in criminal investigations created a 'wall of separation.' That separation effectively forced the Bureau to proceed largely on the criminal justice track if it wanted to preserve the option of using its law enforcement powers to incapacitate terrorists once they were detected."); Louis J. Freeh, Prepared Testimony before the 9/11 Comm'n, at 14 (Apr. 13, 2004) ("For two decades the Department of Justice constructed the wall between counterintelligence and law enforcement higher and higher to a height that far exceeded common sense and the plain meaning of the underlying 1978 statute."); Robert S. Mueller III, FBI Director, Prepared Statement to 9/11 Comm'n, at 2 (Apr. 14, 2004) ("The legal walls between intelligence and law enforcement operations that handicapped us before 9/11 have been eliminated."); Thomas J. Pickard, Prepared Statement to the 9/11 Comm'n, at 7 (Apr. 13, 2004) (stating that case law "resulted in 'walls' being inserted between intelligence and criminal cases, so that the information could not be shared"); John S. Pistole, Exec. Ass't Director for Counterterrorism/Counterintelligence, FBI, Prepared Statement to 9/11 Comm'n, at 3 (Apr. 14, 2004) ("Before [9/11] . . . due to limitations of the legal 'wall' intelligence agents and criminal investigators working on a terrorist target had to proceed without knowing what the other may have been doing about the same target. In short, we were fighting international terrorism with one arm tied behind our back."); Larry D. Thompson, Prepared Statement to 9/11 Comm'n (Dec. 8, 2003) (unpaginated):

> Before the attacks of September 11th, many provisions of federal law had been interpreted to limit sharply the ability of intelligence investigators to communicate with federal law enforcement officials as well as the ability of federal law-enforcement officers to share terrorism-related information with members of the intelligence community. This metaphorical "wall" between intelligence officials and law enforcement officials often inhibited vital information sharing and coordination.

Id.; *cf.* Stephen J. Schulhofer, Prepared Statement to 9/11 Comm'n (Dec. 8, 2003) (unpaginated) (stating that "legal requirements associated with the FISA 'wall'" were "problematic," but "FBI misconceptions about FISA requirements were more basic and predated tensions related to the wall"). *But see* Janet Reno, Prepared Statement to 9/11 Comm'n, at 5 (Apr. 13, 2004) ("There are simply no walls or restrictions on sharing the vast majority of counterterrorism information."). *All available at* http://www.9-11commission.gov/hearings.

[272] 9/11 Comm'n Staff, *Law Enforcement, Counterterrorism, and Intelligence Collection in the United States Prior to 9/11*, Staff Statement No. 9, at 5 (Apr. 13, 2004); *see also id.* at 7, 11 (describing specific ways that "the wall" hampered counterterrorism investigations); 9/11 Comm'n Staff, *Threats and Responses in 2001*, Staff Statement No. 10, at 11 (Apr. 13, 2004) (including "the wall" among the "significant problems sharing information within the FBI").

Commission: "The single greatest structural cause for September 11 was the wall that segregated criminal investigators and intelligence agents."[273] General Ashcroft also claimed that a member of the 9/11 Commission, Jamie Gorelick, provided the "basic architecture for the wall" in a previously classified memorandum that General Ashcroft declassified for the occasion of his testimony.[274] The 9/11 Commission's final report criticized General Ashcroft's testimony as "not fairly or accurately reflect[ing] the significance of the 1995 documents and their relevance to" the events in 2001 that produced the dire e-mail from a New York FBI agent reproduced above.[275]

The Commission's final report also makes clear, however, that the wall played a role in the government's failure to prevent the 9/11 attacks. The report identifies several "missed opportunities to thwart the 9/11 plot."[276] Several of those opportunities involved picking up the trail of two of the 9/11 hijackers, Khalid al Mihdhar and Nawaf al Hazmi, before 9/11.[277] One such opportunity arose at a meeting on June 11, 2001, between a CIA analyst and FBI agents, including an agent whom the Commission Report calls "Jane."[278] Jane did not give her fellow FBI agents "significant" information about one of the future hijackers because she had gotten the information from reports of the National Security Agency (NSA).[279] The NSA reports "contained caveats that their contents could not be shared with criminal investigators [of the FBI]" without the permission of the Justice Department's OIPR. Therefore, 'Jane' concluded that she could not pass on information from those reports to the agents."[280]

---

[273] Testimony of Attorney General John Ashcroft before the National Commission on Terrorist Attacks Upon the United States (Apr. 13, 2004) (unpaginated).

[274] *Id.; see also* Memorandum from Jamie S. Gorelick, Deputy Attorney General on Instructions on "Separation of Certain Foreign Counterintelligence and Criminal Investigations," (undated), *available at* http://www.cnsnews.com/pdf/2004/secret_final2.pdf; Jamie S. Gorelick, "The Truth About the Wall," WASH POST, Apr. 18, 2004, at B07 (saying that memo was written in March 1995).

[275] 9/11 COMM'N REPORT, *supra* note 2, at 539 n.83.

[276] *Id.* at 353; *see also id.* at 355–56 (table of "Operational Opportunities").

[277] *See id.* at 266 ("On four occasions in 2001, the CIA, the FBI, or both had apparent opportunities to refocus on the significance of Hazmi and Mihdhar and reinvigorate the search for them."); *see also id.* at 239 (reproducing photos of al Hazmi and al Mihdhar, and identifying them as members of group that hijacked American Airlines Flight 77, which crashed into Pentagon, *id.* at 10).

[278] *Id.* at 268; *see also id.* at 356 (listing as 6th missed "Operational Opportunity": "FBI and CIA officials do not ensure that all relevant information regarding the Kuala Lumpur meeting was shared with the *Cole* investigators at the June 11 meeting.").

[279] *Id.* at 269. The information concerned a meeting in Kuala Lumpur attended by the two future hijackers, among others. *See id.* at 158–59, 181, 215, and 266–67.

[280] *Id.* at 269.

This is one incident the 9/11 Commission apparently had in mind when it says that, because of the wall, "relevant information from the National Security Agency . . . often failed to make its way to criminal investigators."[281] After the June 11 meeting, Jane refused to let an FBI agent who worked on a criminal investigation in the New York field office participate in the ongoing effort to locate Mihdhar in the United States.[282] That effort relied on intelligence information, which, Jane believed, could be shared only with FBI intelligence agents, and not with FBI criminal agents.[283] Jane's refusal to allow the criminal agent to participate provoked the famous angry e-mail quoted above.[284] The 9/11 Commission found that Jane "appears to have misunderstood the complex rules that could apply to this situation."[285] If so, this reinforces the point that "the wall" resulted not only from the Attorney General's 1995 information sharing procedures but also from the interpretation of those procedures by the FBI, other members of the Department, and the FISA Trial Court.[286]

E. The Patriot Act's Supposed Demolition of the Wall

The 9/11 attacks convinced the Bush Administration to eliminate the primary purpose test and to lower the wall that the Department had built to implement the test. The administration proposed legislation for those purposes less than one week after the attacks.[287] The proposal would have changed one word in the original FISA. The original FISA required the government to certify that "the purpose of the surveillance is to obtain foreign intelligence."[288] As discussed above, this purpose provision in the original FISA was what the lower federal courts had interpreted to impose the primary purpose test.[289] The administration proposed to change the phrase "the purpose" in

---

[281] *Id.* at 79.

[282] *Id* at 271.

[283] *Id.*

[284] *See supra* text accompanying note 267.

[285] 9/11 COMM'N REPORT, *supra* note 2, at 271.

[286] *See also September 11 and the Imperative of Reform in the U.S. Intelligence Community: Additional Views of Sen. Richard C. Shelby, Vice Chairman, Senate Select Comm. On Intelligence* (Dec. 10, 2002) at 46, *available at* http://intellilgence.senate.gov/shelby.pdf ("Much of the blame for the dysfunctional nature of pre-September 11 LEA/IC [Law Enforcement Agency/Intelligence Community] coordination can be traced to a series of misconceptions and mythologies that grew up in connection with the implementation of . . . the Foreign Intelligence Surveillance Act.").

[287] 9/11 COMM'N REPORT, *supra* note 2, at 328.

[288] FISA § 1804(a)(7)(B) (italics added).

[289] *See supra* notes 209–225 and accompanying text.

that provision to "a purpose."[290] The idea was to allow the government to use FISA surveillance for the primary purpose of getting evidence for a prosecution, as long as the gathering of foreign intelligence was also "a" purpose of the surveillance.[291]

The administration's proposed amendment to the original FISA's purpose provision was one of many that the Administration proposed.[292] It got little attention in hearings on the House side.[293] In contrast, some Senators worried about the constitutionality of eliminating the primary purpose test.[294] Their concern was reinforced by opponents of the amendment who doubted its constitutionality.[295]

---

[290] *See Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the Judiciary Comm. of the House of Representatives*, 107th Cong., at 56–57 and 74 (2001) [hereinafter *House Judiciary Hearing on Patriot Act*] (reproducing § 153 of administration's proposed legislation, as well as administration's explanation of this provision, which proposed amendment of FISA § 1804(a)(7)(B)).

[291] *See, e.g., S. 1448, The Intelligence to Prevent Terrorism Act of 2001 and Other Legislative Proposals in the Wake of the September 11, 2001 Attacks: Hearing Before the Senate Select Comm. on Intelligence*, 107th Cong. 53 (2001) [hereinafter *Senate Intelligence Hearing on Patriot Act]* (prepared statement of Jerry Berman, Exec. Dir., Center for Democracy and Technology) ("The proposed provision would permit FISA's use if [foreign intelligence gathering] is 'a' purpose, even if the primary purpose was to gather evidence for a criminal prosecution."); *Protecting Constitutional Freedoms in the Face of Terrorism: Hearing before the Subcomm. on the Constitution, Federalism, and Property Rights of the Senate Judiciary Comm.*, 107th Cong. 18 (2001) [hereinafter *Senate Judiciary Subcomm. Hearing on Patriot Act*] (testimony of Morton H. Halperin, Center for National Security Studies and Council on Foreign Relations) (stating that "the most disturbing" administration proposal "would essentially allow the Justice Department to begin a FISA surveillance even [if] it has already decided that its primary purpose is to develop evidence to indict and convict somebody of a crime and even if that person is a United States citizen"); *see also id.* at 7 (prepared statement of Sen. Sessions) (stating that administration's amendment "would allow, for example, our criminal investigators to assist our intelligence officers in arresting a criminal before he supplies a terrorist with deadly weapons"); *Senate Intelligence Hearing on Patriot Act, supra*, at 22 (testimony of David Kris, Assoc. Deputy Attorney General, U.S. Dep't of Justice) ("What our amendment would do would be to eliminate any artificially high statutory barrier and allow the constitutional standard to be developed on a case-by-case basis.").

[292] *See House Judiciary Hearing on Patriot Act, supra* note 290, at 67–90 (reproducing administration's proposed legislation).

[293] *See id.* at 27 (testimony of Deputy Attorney General Larry D. Thompson explaining proposal); *id.* at 35 (testimony of Assistant Attorney General Michael Chertoff explaining proposal).

[294] *See Senate Intelligence Hearing on Patriot Act, supra* note 291, at 12, 36 (Sept. 24, 2001) (Sen. Edwards' raising question of constitutionality of eliminating primary purpose test); *id.* at 29 (Sen. Feinstein's raising question about constitutionality of eliminating primary purpose test); *id.* at 32 (Sen. DeWine's citing *Keith* and suggesting "real problems" associated with elimination of primary purpose test); *see also id.* at 21 (testimony of David Kris, Assoc. Deputy Attorney General, U.S. Dep't of Justice) (describing constitutionality of proposed elimination of primary purpose test as "a real issue"); *Homeland Defense: Hearing before the Senate Judiciary Comm.*, 107th Cong. 24 (2001) [hereinafter *Senate Judiciary Comm. Hearing on the Patriot Act*] (Sen. Feinstein's saying that "we are concerned that the elimination of the [primary purpose] test might place the FISA in danger of being struck down by a court.").

[295] *See, e.g., Senate Judiciary Subcomm. Hearing on Patriot Act, supra* note 291, at 20

Because of that concern, Senator Feinstein asked Attorney General Ashcroft whether the administration would be satisfied by amending the purpose provision to require "a substantial or significant" purpose to be obtaining foreign intelligence.[296] General Ashcroft seemed amenable.[297]

The bill introduced in Congress as the USA PATRIOT Act proposed to amend the original FISA's purpose provision to require the government to certify that "a significant purpose" of proposed surveillance was to obtain foreign intelligence information. Members of Congress understood that the "significant purpose" language was a compromise.[298] They also understood that it would eliminate the "primary purpose" test.[299] For that reason, some members of Congress suggested that even the compromise version was unconstitutional.[300] Congress nonetheless quickly and

---

(prepared statement of Morton H. Halperin, Center for National Security Studies and Council on Foreign Relations) (stating that administration's amendment to original FISA's purpose provision would allow government to "circumvent[] the notice and probable cause requirements of the Fourth Amendment"); *see also id.* at 28 (prepared statement of Jerry Berman, Exec. Dir., Center for Democracy and Technology) (stating that amendment could cause prosecutions to be "thrown out on constitutional grounds"). *But see id.* at 24 (prepared statement of Prof. John O. McGinnis) (stating that amendment would be constitutional); *id.* at 39 (prepared statement of Prof. Douglas Kmiec) (also stating that amendment would be constitutional).

[296] *Senate Judiciary Comm. Hearing on the Patriot Act*, *supra* note 291, at 24–25.

[297] *Id.* at 35 (testimony of Attorney General John Ashcroft) ("I think . . . we would move toward thinking to say that if 'a purpose' isn't satisfactory [to Congress], say a 'significant purpose' reflects a considered judgment that would be the kind of balancing that I think we are all looking to find."); *see also The USA PATRIOT Act in Practice: Shedding Light on the FISA Process: Hearing before the Senate Judiciary Comm.*, 107th Cong. 7 (2002) [hereinafter cited as *Senate Hearing on the Patriot Act in Practice*] (statement of Sen. Feinstein) (recalling that she had proposed "significant purpose" as a compromise to which General Ashcroft seemed amenable).

[298] *See, e.g.*, 147 CONG. REC. S10,591 (daily ed. Oct. 11, 2001) (statement of Sen. Feinstein) ("The language is a negotiated compromise between those who wished the law to stay the same and those who wished to virtually eliminate the foreign intelligence standard entirely."); 147 CONG. REC. H6759 (daily ed. Oct. 12, 2001) (statement of Sen. Sensenbrenner) (describing "significant purpose" standard as compromise).

[299] *See, e.g.*, 147 CONG. REC. S11,025 (daily ed. Oct. 25, 2001) (statement of Sen. Wellstone) ("The bill broadens the Foreign Intelligence Surveillance Act, FISA, by extending FISA surveillance authority to criminal investigations, even when the primary purpose is not intelligence gathering.").

[300] *See, e.g.*, 147 CONG. REC. S11,021 (daily ed. Oct. 25, 2001) (statement of Sen. Feingold) (by replacing primary purpose test with "significant purpose" provision, "even if the primary purpose is a criminal investigation, the heightened protections of the fourth amendment will not apply"); *id.* at S11,003–04 (statement of Sen. Leahy) (stating that Administration's original proposal "raised constitutional concerns," and that, under the compromise version, providing for "significant purpose" standard, courts would have to decide "how far" the government could go); 147 CONG. REC. S10,558 (daily ed. Oct. 11, 2001) (statement of Sen. Leahy) ("[E]ven the Department [of Justice] concedes that the court's [sic] may impose a constitutional requirement of 'primary purpose' based on the appellate court decisions . . . over the past 20 years."); *id.* at S10,589 (statement of Sen.

overwhelmingly passed the bill of which it was a part.[301]

The Patriot Act included another provision relevant to the primary purpose test. The provision authorizes coordination between officials who conduct FISA surveillance and law enforcement officials:

> (1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title 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 or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.[302]

The provision also specifies that this coordination will not preclude either certification that a significant purpose of the FISA surveillance is to obtain foreign intelligence or the issuance of a surveillance order:

> (2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 1804(a)(7)(B) of this title or the entry of an order under section 1805 of this title.[303]

In sum, Congress amended the original FISA's purpose provision, and added a coordination provision, to eliminate the primary purpose test and lower the wall associated with the test. After Congress enacted the Patriot Act, however, many described the Act as altogether tearing down the wall.[304] Uncertainty about the intent and

---

Edwards) (stating that, while "significant purpose" language was "substantial improvement" of Administration's proposal, FISA Trial Court "will still need to be careful to enter FISA orders only when the requirements of the Constitution as well as the statute are satisfied"); *id.* at S10597 (statement of Sen. Kennedy) (stating that Patriot Act's "significant purpose" amendment "may well make the Foreign Intelligence Surveillance Act unconstitutional under the fourth amendment"); 147 CONG. REC. H6,760 (daily ed. Oct. 12, 2001) (statement of Rep. Scott) (opposing "significant purpose" amendment as one of changes to wiretap law that, "taken together, represent a fundamental attack on principles of privacy").

[301] *See* 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2001), *codified as amended in* Patriot Act § 218. The Patriot Act passed the Senate 98-1 and the House of Representatives 357-66. *See, e.g.*, White House Press Release, Fact Sheet: President Bush Calls for Renewing the USA PATRIOT Act (Apr. 19, 2004), at 2004 WL 61638389.

[302] Patriot Act, § 504(a), 115 Stat. 364 (2001), *codified as amended in* 50 U.S.C. § 1806(k).

[303] *Id.*

[304] *See supra* note 3 and accompanying text.

effect of the Patriot Act on this score developed as the Department of Justice changed its procedures to implement the Patriot Act's changes to the FISA and the courts, in turn, reviewed the Department's efforts. Those events are discussed in the next part of this article.

II. IN RE *SEALED CASE*

A. How the Case Arose

1. The FISA Trial Court Adopts the Attorney General's 1995 Procedures as Required "Minimization Procedures"

In November 2001, a few weeks after Congress enacted the Patriot Act, the FISA Trial Court adopted the Attorney General's 1995 procedures as the required procedures for all future FISA surveillance.[305] This meant that the Attorney General could no longer change those procedures without court approval because they would be incorporated in, and required by, all future surveillance orders issued by the FISA Trial Court.

The FISA Trial Court's action was odd for two reasons. First was its timing. The Attorney General's 1995 procedures implemented the primary purpose test.[306] Yet the FISA Trial Court adopted these procedures as its own after the Patriot Act amended the FISA ostensibly to eliminate the primary purpose test. The court must have known that the Patriot Act was understood to eliminate the primary purpose test; this feature of the Act was widely reported.[307] Also odd was the label that the FISA Trial Court gave its action. The court said

---

[305] *In re* Sealed Case, 310 F.3d. 717, 729 n.17 (Foreign Int. Surv. Ct. Rev. 2002) (noting that the FISA Trial Court adopted part of the 1995 procedures specifically concerning investigations in which FISA surveillance was used).

[306] *See supra* notes 243–262 and accompanying text.

[307] *See, e.g.*, Michael Doyle, *Secret Surveillance Court Raises Fears; Government Given Authority to Wiretap and Search Without Usual Accountability*, SEATTLE POST-INTELLIGENCER, Nov. 5, 2001:

> Congress created the Foreign Intelligence Surveillance Court to ease this tension. Investigators got the secrecy they need, but they also had to keep foreign intelligence collection as the "primary purpose" of the searches.
>
> The new anti-terrorism law, though, expands this so that foreign intelligence need only be a "significant purpose." This seemingly slight shift in wording worries those who fear too many people will be swept up in a law enforcement net.

Id. at A8; Jim McGee, *An Intelligence Giant in the Making: Antiterrorism Law Likely to Bring Domestic Apparatus of Unprecedented Scope*, WASH. POST, Nov. 4, 2001, at A4 (reporting that debate over wording of amendment to original FISA's purpose provision "was one of the fiercest surrounding" the PATRIOT Act).

it was adopting the 1995 procedures as "minimization procedures."[308] The Department had not labeled them such or ever suggested that they were designed as such. Indeed, the Department had a separate set of (classified) procedures that were called "minimization" procedures.[309]

The timing and labeling suggested that the FISA Trial Court wanted to entrench the procedures that established the wall using a statutory basis (the FISA provisions on minimization procedures) that the Patriot Act had not changed.[310] If so, the FISA Trial Court may have been influenced by events besides the enactment of the Patriot Act. Specifically, in 2000 and 2001 the Department of Justice had reported to the FISA Trial Court that many prior FISA applications contained errors and omitted material facts.[311] Almost all of those errors and omissions concerned the Department's compliance with the "wall" procedures.[312] In response, the FISA Trial Court had, in its words, "taken some supervisory actions to assess compliance with the 'wall' procedures."[313] This apparently included disqualifying one FBI agent from involvement in any future FISA applications.[314] The FISA Trial Court's later adoption of the Attorney General's 1995 procedures as the required minimization procedures for all future FISA surveillance may have partly reflected the court's belief that, through systematic violations of the wall procedures, the Department was tearing down the wall even before Congress enacted the Patriot

---

[308] *In re* Sealed Case, 310 F.3d at 729 & n.17.

[309] *Id.* at 728 & n.16.

[310] *Cf.* Banks, *supra* note 30, at 1170 (characterizing FISA Trial Court's reliance on minimization procedures as "tactical judgment" that was "certainly questionable").

[311] FISA Trial Court Opinion, 218 F. Supp. 2d 611, 620–21 (Foreign Int. Surv. Ct. Rev. 2002).

[312] *See* FISA Trial Court Opinion, 218 F. Supp. 2d at 621 ("In virtually every instance, the government's misstatements and omissions in FISA applications and violations of the Court's orders involved information sharing and unauthorized disseminations to criminal investigators and prosecutors."); *see also In re* Sealed Case, 310 F.3d at 730 n.18 (noting that confessed inaccuracies in Department's FISA applications had concerned "assertions regarding the information shared with criminal investigators and prosecutors"). *But cf.* Senators Patrick Leahy, Charles Grassley, and Arlen Specter, *Interim Report on FBI Oversight in the 107th Cong. by the Sen. Judiciary Comm.* at § III.C.2 (Feb. 2003) (finding that FBI's "errors in the 'wall' procedure" was not "the only problem the FBI and DOJ were having in the use of the FISA" and that caused errors and omissions in representations to FISA Trial Court), *available at* http//www.fas.org/irp/congress.2003_rpt/fisa.html.

[313] FISA Trial Court Opinion, 218 F. Supp. 2d at 621.

[314] *See Senate FISA Hearing on the PATRIOT Act in Practice*, *supra* note 297, at 9 (statement of Sen. Specter) (referring to FISA Trial Court's disqualification of FBI agent and expressing frustration that Judiciary Committee could not find out why this happened).

Act to accomplish that result.[315]

2. In 2002, the Department of Justice Changes Information Sharing Procedures To Implement the Patriot Act

In March 2002, Attorney General John Ashcroft issued new "Intelligence Sharing Procedures" to implement the provisions of the Patriot Act that amended the FISA's purpose provision and added the coordination provision.[316] General Ashcroft announced these new procedures in a March 2002 memorandum. The introductory section of the memorandum said that the March 2002 procedures prescribed in the memo superseded the Attorney General's 1995 Procedures on intelligence sharing. The introduction also explained the Department's interpretation of the Patriot Act's effect on the FISA:

> The USA Patriot Act allows FISA to be used for "a significant purpose," rather than the primary purpose, of obtaining foreign intelligence information. Thus, it allows FISA to be used primarily for a law enforcement purpose, as long as a significant foreign intelligence purpose remains.[317]

This explanation treated the Patriot Act as eliminating the primary purpose test. Ironically, though, it also reflected the premise underlying the test by distinguishing "a law enforcement purpose," on the one hand, from "a . . . foreign intelligence purpose," on the other hand. The Department would later persuade the FISA court of review that this distinction was a "false dichotomy."[318]

The March 2002 procedures authorized extensive information sharing between the FBI and the Criminal Division. The procedures said that in general the Division "shall have access to all information" developed in FBI intelligence investigations.[319] To ensure such access, the procedures generally required the FBI to keep the Division

---

[315] *See* Banks, *supra* note 30, at 1171 (stating that FISA Trial Court "reacted to alleged abuses and inadequate management of FISA activities within the Department").

[316] Memorandum from Attorney General on "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI," Mar. 6, 2002, *available at* http://www.fas.prg/irp/agency/doj/fisa/ag03602.html [hereinafter 2002 Att'y Gen. Intelligence Sharing Procedures]; *see also* The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, § VII.B.2, at 25–27 (effective Oct. 31, 2003) (redacted version, reflecting procedures announced in 2002 Att'y Gen. Intelligence Sharing Procedures) [hereinafter cited as 2003 Attorney General Guidelines for FBI National Security Investigations], *available at* http://www.fas.org/irp/agency/doj.fbi.nsiguidelines.pdf.

[317] 2002 Att'y Gen. Intelligence Sharing Procedures, *supra* note 316, § I, reproduced *supra* text accompanying note 246.

[318] *See In re* Sealed Case, 310 F.3d at 735.

[319] 2002 Att'y Gen. Intelligence Sharing Procedures, *supra* note 316, § II.A.

and OIPR "apprised of all information . . . necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities."[320] (This language tracked that of the coordination provision that the Patriot Act had added to the FISA.[321]) In detailing the FBI's obligation, the procedures specified, "Relevant information includes both foreign intelligence information and information concerning a crime which has been, is being, or is about to be committed."[322] This statement distinguishes foreign intelligence information from evidence of crime, again suggesting— as did the introductory section of the memo—the same dichotomy between law enforcement and intelligence functions that underlay the primary purpose test. Even so, the March 2002 procedures greatly relaxed the restrictions that the 1995 procedures had put on the flow of information from the FBI to the Criminal Division.

The March 2002 procedures also relaxed the restrictions that the 1995 procedures had put on the Criminal Division's ability to consult with the FBI. The 1995 procedures had prohibited "the fact or the appearance of the Criminal Division's directing or controlling the FI or FCI investigation toward law enforcement objectives."[323] In contrast, the 2002 Procedures authorized consultations on "the initiation, operation, continuation, or expansion of FISA searches or surveillance."[324] By authorizing the Criminal Division to advise the FBI to "initiat[e]" or "expan[d]" FISA surveillance,[325] the 2002 procedures, unlike the 1995 procedures, allowed at least "the appearance" that the Division was "directing or controlling" FISA surveillance "toward law enforcement objectives."[326]

In addition to the provisions about information sharing and consultation between the FBI and the Criminal Division, the March 2002 procedures opened up the information flow in two other ways. First, they largely eliminated OIPR's role as a gatekeeper.[327] Second,

---

[320] *Id.*

[321] Patriot Act, § 504(a), 115 Stat. 364 (2001), codified as amended in 50 U.S.C. § 1806(k), reproduced *supra* text accompanying note 302-03.

[322] 2002 Att'y Gen. Intelligence Sharing Procedures, *supra* note 316 § II.A.

[323] 1995 Att'y Gen. Procedures, *supra* note 243, at § A.6.

[324] 2002 Att'y Gen. Procedures, *supra* note 316, at § II.B; see also id. § III (generally authorizing U.S. Attorney's Offices to receive information and engage in consultations to same extent as Criminal Division lawyers were authorized to do under § II).

[325] *Id.*

[326] 1995 Att'y Gen. Procedures, *supra* note 243, at § A.6.

[327] 2002 Att'y Gen. Procedures, *supra* note 316, § II.B (providing that FBI and Criminal Division could consult directly without OIPR's presence).

they allowed the U.S. Attorneys' Offices to "receive information and engage in consultations to the same extent as the Criminal Division."[328] Under the 1995 procedures, in contrast, the FBI needed the Criminal Division's advance approval to contact a U.S. Attorney's Office about any investigation that included FISA surveillance.[329] The March 2002 procedures would precipitate a showdown between the Department and the FISA Trial Court.

3. The FISA Trial Court Rejects the Department's March 2002 Information Sharing Procedures

The day after Attorney General Ashcroft announced the March 2002 intelligence sharing procedures, the Department responded to the FISA Trial Court's order (issued four months earlier) adopting the now-superseded 1995 procedures as court-required minimization procedures. The Department filed a motion, accompanied by a copy of the March 2002 procedures, "to vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including this Court's adoption of the Attorney General's July 1995 intelligence sharing procedures, which are not consistent with new intelligence sharing procedures submitted for approval with this motion."[330]

In May 2002, the FISA Trial Court issued an opinion and order on the motion. The opinion was written by the outgoing Chief Judge of the FISA Trial Court (and longtime Justice Department official), Royce Lamberth.[331] The opinion indicated that "[a]ll seven judges of the Court concur[red]" in the opinion.[332] The court described its disposition of the government's motion in a way that implied a government victory: "The Government's motion will be GRANTED, EXCEPT THAT THE PROCEDURES MUST BE MODIFIED IN PART." Really, the decision was at most only a partial win for the government, and only in its result, not its reasoning. The result was that the court accepted the portion of the government's March 2002 procedures that governed information sharing.[333] The court largely rejected, however, the portion of the March 2002 procedures governing consultation between the Criminal Division and the FBI.

---

[328] *Id.* at § III.

[329] 1995 Att'y Gen. Procedures, *supra* note 243, at § A.2.

[330] FISA Trial Court Opinion, 218 F. Supp. 2d 611, 613 (Foreign Int. Surv. Ct. Rev. 2002).

[331] *Id.*; *see also* Almanac of the Federal Judiciary (entry on Royce C. Lamberth), *available at* 2002 WL 32050752.

[332] FISA Trial Court Opinion, 218 F. Supp. 2d at 625.

[333] *See id.*

The court replaced that portion of the procedures with restrictions derived from the superseded 1995 procedures.[334] Beyond that result, the court's reasoning reaffirmed the "primary purpose" test while tracing it to a new place: not the FISA's "purpose" provision, but its provisions on "minimization procedures."

As a predicate for this new approach, the FISA Trial Court found that the Attorney General's March 2002 procedures were minimization procedures (though the Department had not called them such).[335] The court relied on the FISA's definition of "minimization procedures" to reject the procedures.[336] Specifically, the court determined that the procedures were "designed to enhance the acquisition, retention, and dissemination of *evidence for law enforcement purposes, instead* of being consistent with the need of the United States to 'obtain, produce, and disseminate *foreign intelligence information*.'"[337] Their design reflected the government's position that the FISA "may now be used *primarily* for a law enforcement purpose."[338] In the court's view, the 2002 procedures thus made the government's interest in foreign intelligence gathering "*subordinat[e]*" to "law enforcement objectives."[339] For that reason, the 2002 procedures were not "'consistent' with the need to obtain, produce, and disseminate *foreign intelligence information*."[340]

---

[334] As modified, the procedures specifically prohibited—instead of specifically authorizing—"law enforcement officials" from "mak[ing] recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches and surveillance." *See id.*; *cf.* 2002 Att'y Gen. Procedures, *supra* note 316, at § II.B, III (reproduced in relevant part in text accompanying note 324 *supra*). Further, the court's modification added these injunctions: "[T]he FBI and the Criminal Division shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillance toward law enforcement objectives." FISA Trial Court Opinion, 218 F. Supp. 2d at 625. The court's modifications also added a new provision, which the government dubbed "the chaperone requirement." It required that OIPR be invited to all consultations between the FBI and the Criminal Division; if OIPR could not attend, "OIPR shall be apprised of the substance of the consultations forthwith in writing so that the Court may be notified at the earliest opportunity." *Id.* Finally, "to monitor compliance" with these requirements, the FISA Trial Court adopted a "new administrative rule," designated Rule 11, which required all FISA applications to "include informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors at the Department of Justice or a United States Attorney's Office." *Id.* at 627.

[335] *Id.* at 616.

[336] *Id.*

[337] *Id.* at 623 (quoting 50 U.S.C. §§ 1801(h) and 1821(4)) (emphasis added by the FISA Trial Court).

[338] *Id.* (internal quotation marks omitted).

[339] *Id.* at 623–24.

[340] *Id.* at 622.

4. The Department of Justice Creates a Route for Appealing the FISA Trial Court's Opinion

The FISA Trial Court's May 2002 ruling was probably not appealable. The court had ruled on a procedural motion by the government—not on an application for a surveillance order. The FISA authorizes appellate review only of "the denial of an[] application" by the FISA Trial Court.[341] Apparently to create a route for appealing the May 2002, ruling, the government later applied for a FISA surveillance order that did not include the "minimization procedures" that the court had prescribed in the May 2002 decision.[342] The FISA Trial Court granted the application only after modifying it to include the procedures that it had prescribed in that decision.[343] The court did the same thing when the government applied to have the order renewed without the prior modifications.[344] The government then appealed on the ground that the court had partially denied the original and renewal applications. The FISA Court of Review took jurisdiction.[345]

B. The FISA Court of Review's Opinion

On appeal, the government made two arguments of statutory interpretation. It argued, first, that the original FISA did not impose the "primary purpose" test; the test was invented by some lower federal courts based on a supposed "dichotomy" between foreign intelligence and law enforcement.[346] Second, the government argued, even if the original FISA imposed a primary purpose test, the Patriot Act amendments eliminated that test.[347] In addition to these statutory arguments, the government argued that, as amended by the Patriot Act, the FISA does not violate the Fourth Amendment, because the Fourth Amendment does not, of its own force, compel the primary purpose test for FISA surveillance.[348] Two amicus groups, the

---

[341] 50 U.S.C. § 1803(b).

[342] *In re* Sealed Case, 310 F.3d at 720–21 & n.4.

[343] *Id.* at 720.

[344] *Id.* at 720 n.4.

[345] *Id.* at 721.

[346] *Id.*; *see also* Brief for the United States at 8, *In re* Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002) (No. 02-001) [hereinafter Principal Brief for U.S., *In re* Sealed Case]; Supplemental Brief for the United States, at 1, *In re* Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002) (No. 02-001).

[347] Principal Brief for U.S., *In re* Sealed Case, *supra* note 346, at 12–26.

[348] *See In re* Sealed Case, 310 F.3d at 722; *see also* Supplemental Brief for the United States, *supra* note 346, at 17–23; Principal Brief for U.S., *In re* Sealed Case, *supra* note 346, at 26–32.

American Civil Liberties Union and the National Association of Criminal Defense Lawyers, argued that the FISA violates the Fourth Amendment unless it is construed to impose the primary purpose test.[349]

The FISA Court of Review ruled mostly in favor of the government. Its rulings on the original FISA; the FISA as amended by the Patriot Act; and the Fourth Amendment are discussed separately below.

1. The Court of Review's Analysis of the Original FISA

The Court of Review agreed with the government that the original FISA did not impose the primary purpose test.[350] The court determined that the test rests on a dichotomy between gathering foreign intelligence on one hand, and investigating and prosecuting crime, on the other.[351] The court found no basis for this dichotomy in the text or the legislative history of the FISA. The court did, however, construe the original FISA to restrict the government's use of FISA surveillance for prosecutorial purposes.

The court found the text and legislative history of the original FISA incompatible with the dichotomy on which the primary purpose test is premised. Far from distinguishing foreign intelligence information from evidence of crime, the text of the FISA defined "foreign intelligence information" to "include[] evidence of crimes such as espionage, sabotage [and] terrorism."[352] Indeed, the definition as applied to U.S. persons "is grounded on criminal conduct."[353] Moreover, the legislative history confirmed Congress's understanding and intent that "foreign intelligence information" would include "evidence of certain crimes":

> [T]he term "foreign intelligence information," especially as defined in subparagraphs (e)(1)(B) and (e)(1)(C), can include evidence of certain crimes relating to sabotage, international terrorism, or clandestine intelligence activities. With respect to information concerning U.S. persons, foreign intelligence information includes information necessary to protect against clandestine intelligence activities of foreign powers or their agents. Information about a spy's espionage activities obviously is within

---

[349] *In re* Sealed Case, 310 F.3d at 722.

[350] *See id.* at 723–24 (discussing purpose provision); *id.* at 730–31 (discussing minimization procedures).

[351] *See id.* at 727.

[352] *Id.* at 723.

[353] *Id.* at 723.

> this definition, and it is most likely at the same time evidence of criminal activities.[354]

The Court of Review admitted that some legislative history supported the primary purpose test. For example, a House report said that FISA surveillances "are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information."[355] The court found that this statement "was an observation, not a proscription."[356]

In addition to finding congressional recognition that foreign intelligence information can include evidence of crime, the Court of Review found support for the government's argument on the instrumental connection between prosecution and foreign intelligence purposes. The government argued that "arresting and prosecuting terrorist agents of, or spies for, a foreign power may well be the best technique to prevent them from successfully continuing their terrorist or espionage activity."[357] The court determined that "Congress actually anticipated" this argument "and explicitly approved it" in the legislative history. A House report said:

> How this information may be used to protect against 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 . . . . And no information acquired pursuant to this bill could be used for other than lawful purposes . . . . Obviously, use of "foreign intelligence information" as evidence in a criminal trial is 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 [these activities] can be sought, retained, and used pursuant to this bill.[358]

A Senate report was "on all fours" with the House report,[359] stating:

> 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, kidnaping, and terrorist acts committed by or on behalf of foreign powers. Intelligence and criminal law

---

[354] *Id.* at 724 (quoting H.R. REP. NO. 95-1283, pt. 1, at 49 (1978)).

[355] *Id.* at 725 (quoting H.R. REP. NO. 95-1283, pt. 1, at 36 (1978)).

[356] *Id.*

[357] *Id.* at 724.

[358] *Id.* at 724–25 (quoting H.R. REP. NO. 95-1283, pt. 1, at 49 (1978)) (emphasis in original).

[359] *Id.* at 725.

> enforcement tend to merge in this area . . . . [S]urveillances 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.[360]

The court concluded from the text and legislative history of the FISA that the original FISA "did not impose any restrictions on the government's use of foreign intelligence information to prosecute agents of foreign powers for foreign intelligence crimes."[361] The court defined "foreign intelligence crimes" primarily to mean the crimes to which the definition of "agent of a foreign power" (as applied to U.S. persons) refers.[362]

The court did not believe, however, that the original FISA allowed the government to use FISA surveillance to get evidence of "non-foreign intelligence crimes."[363] Acknowledging the government's argument that even prosecution of non-foreign intelligence crimes by foreign agents could "stop espionage or terrorism by putting [the agent] in prison,"[364] the court nonetheless concluded that the government's argument "transgresses the original FISA."[365] The court identified the specific FISA provision precluding the government's argument as the provision requiring the government to certify that "the purpose" of the proposed surveillance was "to obtain foreign intelligence information."[366] House Report statements confirmed the court's interpretation of the purpose provision, namely that it served to:

> prevent the practice of targeting, for example, a foreign power for electronic surveillance when the true purpose of the surveillance is to gather information about an individual for other than foreign intelligence purposes. It is also designed to make explicit that the sole purpose of such surveillance is to secure "foreign intelligence information," as defined, and not to obtain some other type of

---

[360] *Id.* (quoting S. REP. NO. 95-701, at 10–11 (1978)) (alteration in original).

[361] *Id.*

[362] *Id.* at 723; *see also id.* at 723 n.10 (noting that "foreign intelligence crimes" referred not only to crimes identified in the FISA definition of "agent of a foreign power," but also to entering the United States under a false or fraudulent identity or on behalf of a foreign power, *see* 50 U.S.C. § 1801(b)(2)(C) (2000), "which will almost always involve a crime"); *cf. id.* at 736 (explaining that "foreign intelligence crimes" also include "ordinary crimes . . . inextricably intertwined with foreign intelligence crimes").

[363] *Id.* at 735–36.

[364] *Id.* at 736.

[365] *Id.*

[366] Foreign Intelligence Surveillance Act § 104(a)(7)(B), 50 U.S.C. § 1804(a)(7)(B) (2000).

information.[367]

The court understood this passage to "prevent the government from targeting a foreign agent when its 'true purpose' was to gain non-foreign intelligence information, such as evidence of ordinary crimes or scandals."[368] The court recognized that "ordinary crimes might be inextricably intertwined with foreign intelligence crimes,"[369] The court explained that, accordingly, "ordinary crimes" could sometimes be treated like "foreign intelligence crimes." "For example, if a group of international terrorists were to engage in bank robberies in order to finance the manufacture of a bomb, evidence of the bank robbery should be treated just as evidence of the terrorist act itself."[370] "But," the court added, "the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes."[371] Thus, the Court of Review concluded that evidence of "wholly unrelated ordinary crime" is not "foreign intelligence information," even if the government intends to use the evidence to stop a foreign threat.

2. The Court of Review's Analysis of the Patriot Act Amendments to the FISA

The court observed that after 9/11 the government sought an amendment of the FISA "in order to avoid the requirement of meeting the 'primary purpose' test."[372] Congress responded in the Patriot Act with "language which [Congress] perceived as not giving the government quite the degree of modification it wanted."[373] As amended by the Patriot Act, the FISA required the government to certify that "a significant purpose" (rather than merely "a purpose") of proposed surveillance is to obtain foreign intelligence information.

The Court of Review found that Congress knew that the "significant purpose" amendment would "relax[] a requirement that the government show that its primary purpose was other than criminal prosecution."[374] The court quoted Senator Patrick Leahy, then chairman of the Senate Judiciary Committee, who said, "This bill . . .

---

[367] *In re* Sealed Case, 310 F.3d at 725 (quoting H.R. REP. NO. 95-1283, pt. 1, at 76 (1978)); *see also id.* at 736.
[368] *Id.* at 736 (quoting H.R. REP. NO. 95-1283, pt. 1, at 76 (1978)).
[369] *Id.*
[370] *Id.*
[371] *Id.*
[372] *Id.* at 732.
[373] *Id.*
[374] *Id.*

break[s] down traditional barriers between law enforcement and foreign intelligence . . . ."[375] Specifically relevant to the primary purpose test, Senator Leahy considered it "very problematic" that the Patriot Act would "make it easier for the FBI to use a FISA wiretap . . . where the government's most important motivation for the wiretap is for use in a criminal prosecution."[376] The Court of Review also cited the floor statement of Senator Dianne Feinstein, member of both the Senate Intelligence and Judiciary Committees, where she proclaimed that the Patriot Act would make it "easier to collect foreign intelligence . . . under the [FISA]."[377] Elaborating on the need for such change, Senator Feinstein explained:

> Under current law, authorities can proceed with surveillance under FISA only if the primary purpose of the investigation is to collect foreign intelligence . . . . Determining which purpose is the "primary" purpose of the investigation can be difficult . . . . Rather than forcing law enforcement to decide which purpose is primary, law enforcement or foreign intelligence gathering, this bill strikes a new balance. It will now require that a "significant" purpose of the investigation must be foreign intelligence gathering to proceed with surveillance under FISA. The effect of this provision will be to make it easier for law enforcement to obtain a FISA search or surveillance warrant for those cases where the subject of the surveillance is both a potential source of valuable intelligence and the potential target of a criminal prosecution.[378]

Additionally, the court quoted Patriot Act opponent and Judiciary Committee member Senator Russell Feingold, who warned that the "significant purpose" amendment would let the government get a FISA surveillance order "even if the primary purpose is criminal investigation."[379] In Senator Feingold's view, this violated the Fourth Amendment.[380] To the FISA Court of Review, these statements, combined with the addition of section 1806(k), which expressly sanctioned coordination between law enforcement and foreign

---

[375] *Id.* (quoting 147 CONG. REC. S10992 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy)).

[376] *Id.* at 733 (quoting 147 CONG. REC. S10593 (daily ed. Oct. 11, 2001) (statement of Sen. Leahy)).

[377] *Id.* at 732 (quoting 147 CONG. REC. S10591 (daily ed. Oct. 11, 2001) (statement of Sen. Feinstein)).

[378] *Id.* at 732–33 (quoting 147 CONG. REC. S10591 (daily ed. Oct. 11, 2001) (statement of Sen. Feinstein)).

[379] *Id.* at 733 (quoting 147 CONG. REC. S11021 (daily ed. Oct. 25, 2001) (statement of Sen. Feingold)).

[380] *Id.* (quoting 147 CONG. REC. S11021 (daily ed. Oct. 25, 2001) (statement of Sen. Feingold)).

intelligence officials, proved that "the Patriot Act amendments [to the original FISA] clearly disapprove the primary purpose test."[381]

Having held that, as amended by the Patriot Act, the FISA allowed the government to use FISA surveillance for the "primary purpose" of prosecution, the Court of Review's reasoning then took a somewhat surprising turn:

> [A]s a matter of straightforward logic, if a FISA application can be granted even if "foreign intelligence" is only a significant—not a primary—purpose, another purpose can be primary. One other legitimate purpose that could exist is to prosecute a target for a foreign intelligence crime. We therefore believe the Patriot Act amply supports the government's . . . argument [that the Patriot Act eliminated the primary purpose test] but, paradoxically, the Patriot Act would seem to conflict with the government's . . . argument [that the dichotomy between foreign intelligence and law enforcement is false] because by using the term "significant purpose," the Act now implies that another purpose is to be distinguished from a foreign intelligence purpose.[382]

Thus, the court determined that the Patriot Act's "significant purpose" amendment caused the FISA, for the first time, to distinguish between foreign intelligence and law enforcement:

> In short, even though we agree that the original FISA did not contemplate the "false dichotomy," the Patriot Act actually did, which makes it no longer false. The addition of the word "significant" to section 1804(a)(7)(B) imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes.[383]

The court believed that this change reflected a broader change—namely, that it allowed FISA judges, for the first time, to review the government's intended use of information obtained by FISA surveillance:

> Although section 1805(a)(5) [providing for judicial review of the certifications in an application for FISA surveillance] . . . may well have been intended to authorize the FISA court to review only the question whether the information sought was a type of foreign intelligence information, in light of the significant purpose amendment of section 1804 it seems section 1805 must be interpreted as giving the FISA court the authority to review the

---

[381] *Id.* at 734.
[382] *Id.*
[383] *Id.* at 735.

government's purpose in seeking the information.[384]

This reasoning left the Court of Review with "something of an analytic conundrum."[385] On the one hand, the Patriot Act did not amend the FISA definition of "foreign intelligence information."[386] With respect to U.S. persons, that definition therefore continues to include much information that is evidence of a crime.[387] On the other hand, the court recognized that Congress "accepted the dichotomy between foreign intelligence and law enforcement by adopting the significant purpose test."[388] To resolve the conundrum, the Court articulated three principles for FISA surveillance orders targeting U.S. persons.

First, the government can use FISA surveillance for the primary purpose of investigating and prosecuting "foreign intelligence crimes."[389] This first principle reflects that Congress intended the Patriot Act to relax the judicially developed "primary purpose" test.[390]

The second principle qualifies the first principle: The government cannot get a FISA surveillance order if its *sole* purpose is to gather evidence for a prosecution, even the prosecution of foreign intelligence crimes.[391] In the court's view, the FISA as amended by the Patriot Act "excludes from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution."[392] Accordingly, the court distinguishes the purpose of obtaining foreign intelligence information from the purpose of obtaining evidence for criminal prosecution.[393] Granting the difference, if the government's sole purpose is to build a prosecution—even the prosecution of a foreign intelligence crime—the government cannot certify, as the FISA requires, that a "significant" purpose is obtaining foreign intelligence. The Court of Review explained, "The addition of the word 'significant' to section 1804(a)(7)(B) imposed a requirement

---

[384] *Id.*

[385] *Id.*

[386] *Id.*

[387] *See id.*; *see also supra* notes 98–102, 129 and accompanying text (discussing the FISA's definition of foreign intelligence information).

[388] *Id.*

[389] *See id.*

[390] *See id.* at 734.

[391] *See id.* at 735.

[392] *Id.*

[393] *See id.* ("Congress accepted the dichotomy between foreign intelligence and law enforcement.").

that the government have a measurable foreign intelligence purpose, *other than* just criminal prosecution of even foreign intelligence crimes."[394]

The court did not think this second principle would "make much practical difference":

> [W]hen [the government] commences an electronic surveillance of a foreign agent, typically it will not have decided whether to prosecute the agent (whatever may be the subjective intent of the investigators or lawyers who initiate an investigation). So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test.[395]

The court also reiterated, however, that if "the government's sole objective [is] merely to gain evidence of past criminal conduct—even foreign intelligence crimes—to punish the [foreign] agent rather than halt ongoing espionage or terrorist activity, the application [for FISA surveillance] should be denied."[396]

The third principle is that the government cannot get a FISA surveillance order if it has "a primary objective of prosecuting an agent for a non-foreign intelligence crime."[397] The court traced this principle to the original FISA.[398] The court read the legislative history of the original FISA as precluding the use of FISA when the government's "'true purpose' [is] to gain non-foreign intelligence information—such as evidence of ordinary crimes or scandals."[399] The court interpreted the term "foreign intelligence information" generally to exclude "evidence of ordinary crime," even if, as the government argued, the prosecution of such crime would serve a foreign intelligence purpose such as "stopping espionage or terrorism by putting an agent of a foreign power in prison."[400] In the court's view, the original FISA permitted the government to use FISA-acquired evidence to prosecute "ordinary crime" only if the government "inadvertently came upon" the evidence.[401] The court

---

[394] *Id.* (emphasis added).
[395] *Id.*
[396] *Id.*
[397] *Id.* at 736.
[398] *Id.* (holding that government's interpretation permitting prosecution of even non-foreign intelligence crimes so long as the prosecution served a foreign intelligence purpose "transgresses the original FISA").
[399] *Id.* (quoting H.R. REP. NO. 95-1283, pt. 1, at 76 (1978)).
[400] *Id.*
[401] *Id.*

acknowledged that, by amending the original FISA's purpose provision, the Patriot Act arguably permits the government to use FISA surveillance for the primary purpose of prosecuting non-foreign intelligence crimes as long as the government also has some other purpose in mind that is "significant" and related to collection of foreign intelligence.[402] The court dismissed that, however, as "an anomalous reading of the amendment."[403]

The court did not define the "non-foreign intelligence crimes" that, under its third principle, the government cannot use FISA surveillance for the primary (much less the sole) purpose of obtaining.[404] The court suggested, though, that the term excludes both what it had previously defined as "foreign intelligence crimes," as well as otherwise "ordinary" crimes that, in a particular case, are "inextricably intertwined with foreign intelligence crimes":[405]

> For example, if a group of international terrorists were to engage in bank robberies in order to finance the manufacture of a bomb, evidence of the bank robbery should be treated just as evidence of the terrorist act itself. But the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.[406]

The Court of Review realized that its decision required FISA judges to review the government's purpose in applying for FISA surveillance orders, as courts did under the "primary purpose" test. Accordingly, the court cautioned:

> [T]he government's purpose as set forth in a section 1804(a)(7)(B) certification is to be 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. It is up to the Director of the FBI, who typically certifies, to determine the government's national security purpose, as approved by the Attorney General or Deputy Attorney General.[407]

In particular, the court warned that a FISA judge should not gauge the government's purpose "by seeking to inquire into which Justice Department officials were instigators of an investigation."[408] Instead, "the relevant purpose is that of those senior officials in the Executive Branch who have the responsibility of appraising the government's

---

[402] *Id.*
[403] *Id.*
[404] *Id.*
[405] *Id.*
[406] *Id.*
[407] *Id.*
[408] *Id.*

national security needs."[409]

3. The Court of Review's Fourth Amendment Ruling

The Court of Review's statutory interpretation raised a constitutional issue. Specifically, the Court interpreted the Patriot Act to replace the judicially created "primary purpose" test with a "significant purpose" test. Other courts, however, had construed the FISA to incorporate the primary purpose test as a Fourth Amendment requirement for surveillance under the FISA to be valid.[410] Having construed the Patriot Act to eliminate that test from the FISA, the Court of Review addressed whether, so construed, the FISA violates the Fourth Amendment.[411]

The court held that the FISA satisfies the Fourth Amendment.[412] In so holding, the court found it unnecessary to resolve the case under the warrant clause of the Fourth Amendment. Looking instead to the reasonableness clause of that Amendment, the court held that electronic surveillance under the FISA, as amended by the Patriot Act and as interpreted by the Court of Review, is "reasonable."[413]

4. Summary of Court of Review's Opinion; Description of That Court's Disposition of the Case; Later Proceedings in the Case

Overall, the FISA Court of Review's decision produced a favorable outcome for the federal government. True, the court did interpret the Patriot Act's amendment of the FISA to put two restrictions on FISA surveillance: The government cannot use it (1) for the sole purpose of investigating or prosecuting crime, even foreign intelligence crimes; or (2) for the primary (or sole) purpose of investigating or prosecuting non-foreign intelligence related crimes. However, the Court of Review interpreted the Patriot Act to replace the primary purpose test with a less demanding "significant purpose" test. So interpreted, the court found that the FISA satisfies the Fourth Amendment.[414]

---

[409] *Id.*

[410] *See supra* notes 210–23 and accompanying text.

[411] *In re* Sealed Case, 310 F.3d at 719 n.1. Proceedings concerning applications for FISA surveillance orders are *ex parte. See supra* note 78 and accompanying text.

[412] *See id.* at 736–46.

[413] *See id.* at 742–46; *see also* Principal Brief for the United States at 30, *In re* Sealed Case, 310 F.3d 717 ("Even if *Truong* was correctly decided, and the Constitution requires a 'primary' intelligence purpose for unilateral Executive Branch surveillance, a 'significant' intelligence purpose for FISA surveillance conducted with the prior approval of an Article III court would be reasonable and therefore constitutional under the Fourth Amendment.").

[414] The FISA Court of Review took three steps to dispose of the case: (1) It reversed the

The Court of Review's decision became the final decision in the case. The federal government did not seek review in the U.S. Supreme Court and could not have done so, having won the judgment.[415] Supreme Court review was sought, however, by two of the groups participating as amici curiae in the Court of Review, joined by other groups. They moved in the Supreme Court for leave to intervene and to file a petition for a writ of certiorari;[416] this was summarily denied in March 2003.[417]

III. ANALYSIS OF STATUTORY ISSUES AND THEIR TREATMENT BY THE FISA COURTS

The FISA Court of Review came to an admittedly "paradoxical" conclusion.[418] The Patriot Act was supposed to expand the government's power to combat international terrorism and other foreign threats. The Court of Review, however, construed the Act to restrict that power by creating, for the first time, a statutory basis for distinguishing between foreign intelligence purposes and law enforcement purposes. According to the court, it was the Patriot Act, not the original FISA, in which "Congress accepted the dichotomy between foreign intelligence and law enforcement."[419] This Part of the article analyzes that interpretation, building on the explication in

---

FISA Trial Court's orders "to the extent they imposed conditions on the grant of the government's applications"; (2) it remanded the case "with instructions to grant the [government's] applications [for FISA surveillance] as submitted"; and (3) it vacated the FISA Trial Court's "Rule 11." *In re* Sealed Case, 310 F.3d at 746; *see also supra* note 334 and accompanying text (describing Rule 11).

[415] The FISA authorizes U.S. Supreme Court review if the FISA Court of Review "determines that [a government] . . . application [for an order approving FISA surveillance] was properly denied [by the FISA Trial Court]." That situation did not occur in *In re* Sealed Case, where the FISA Court of Review determined that the government's applications for FISA surveillance orders were *improperly* denied (in part) by the FISA Trial Court. Moreover, the government won the judgment in the FISA Court of Review. That court entered a judgment reversing the FISA Trial Court judgment and remanding the case with instructions to grant the government's applications. True, the FISA Court of Review articulated two restrictions on the government's use of FISA surveillance. *See supra* notes 391–406 and accompanying text. Since the portion of the court's decision doing so was not necessary to the judgment, however, it is dicta and, as such, is not subject to Supreme Court review at the instance of the government as the judgment winner. *See, e.g.*, Black v. Cutter Labs., 351 U.S. 292, 297 (1956) ("This Court . . . reviews judgments, not statements in opinions.").

[416] *See* Petition of American Civil Liberties Union [ACLU] et al. for Leave to Intervene and Petition for a Writ of Certiorari, *In re* Sealed Case, *available at* http://www.aclu.org/Files/OpenFile.cfm?id=11838 (last visited November 23, 2004); Petition of ACLU et al. for a Writ of Certiorari, *In re* Sealed Case, *available at* http://www.aclu.org/Files/OpenFile.cfm?id=11836 (last visited Nov. 23, 2004).

[417] American Civil Liberties Union v. United States, 538 U.S. 920 (2003).

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

[419] *Id.* at 735.

Part I of the relevant statutory language and the identification in Part II of some of the relevant legislative history. This Part concludes that the Court of Review incorrectly interpreted both the original FISA and the FISA as amended by the Patriot Act. But so did the FISA Trial Court when it interpreted the FISA, as amended by the Patriot Act, to retain the primary purpose test, and so did the federal courts of appeals that interpreted the original FISA to impose the primary purpose test. This article respectfully contends that all of this precedent is mistaken.

First, Section A below explains why these issues of statutory interpretation are important. In a nutshell, they are important because the meaning of FISA is intertwined with the Fourth Amendment issue, and Congress is fast approaching a deadline for deciding which version of the FISA, if any, will stay on the books. Furthermore, whatever Congress does (or fails to do), courts in current and future prosecutions will have to address the legality of the surveillance that is occurring under the current version of FISA and is producing evidence of crime.

Section B analyzes the original FISA. The analysis shows that the original FISA did not impose the primary purpose test. The original FISA did, however, require the government to intend to use foreign intelligence information obtained under FISA surveillance for one or more of five foreign intelligence purposes specified in the FISA's definition of "foreign intelligence information." Thus, the FISA Court of Review was right—and other federal courts of appeals (as well as the FISA Trial Court) have been wrong—in deciding that the original FISA did not impose the primary purpose test. The FISA Court of Review was wrong, however, in interpreting the original FISA not to impose any limit on the government's use of foreign intelligence information to prosecute "foreign intelligence crimes." In short, the original FISA was more restrictive of FISA surveillance than the Court of Review determined.

In contrast, Section C concludes that, as amended by the Patriot Act, the FISA is less restrictive than the Court of Review determined. The current FISA does not impose either of the restrictions that the Court of Review discerned. Thus, the FISA allows the government to use FISA surveillance for the sole purpose of prosecuting a foreign intelligence crime. Furthermore, the government can use FISA surveillance for the primary (or sole) purpose of prosecuting "ordinary crime." Prosecutorial use of FISA surveillance is permissible as long as the government intends the prosecution to

serve a foreign intelligence purpose.

A. Importance of Statutory Rulings in In re Sealed Case

The Chairman of the Senate Judiciary Committee called the FISA Trial Court's decision in In re Sealed Case "one of the most important legal opinions in the last 20 years of national security law" when opening a hearing devoted to the case.[420] The Court of Review's decision reversing the FISA Trial Court is likewise a "landmark" opinion[421] addressing "one of the most important" provisions in the Patriot Act.[422] The decisions have not received much scholarly commentary, however, and most scholarly commentary that does exist focuses on the Fourth Amendment issues posed by FISA surveillance, rather than the statutory issues.[423] The statutory issues deserve attention, however, for three reasons.

First, the statutory issues affect the existence and nature of the Fourth Amendment issues. The central Fourth Amendment issue is whether the Fourth Amendment requires FISA surveillance to meet the "primary purpose" test of *Truong*.[424] That issue arises, however, only if the FISA does not of its own force impose the test.[425] Thus, the FISA Trial Court did not address the Fourth Amendment issue

---

[420] *Senate Hearing on the Patriot Act in Practice, supra* note 297, (statement of Sen. Leahy), *available at* http://judiciary.senate.gov/member_statement.cfm?id=398&wit_id=50; *see also* Senators Patrick Leahy, Charles Grassley, and Arlen Specter, *Interim Report on FBI Oversight in the 107th Cong. by the Sen. Judiciary Comm.* at § II.B.1 (Feb. 2003) (describing FISA Trial Court opinion as a "landmark legal opinion"), *available at* http://www.fas.org/irp/congress.2003_rpt/fisa.html (last visited Nov. 23, 2004).

[421] *September 11 and the Imperative of Reform in the U.S. Intelligence Community: Additional Views of Sen. Richard C. Shelby, Vice Chairman, Senate Select Comm. on Intelligence* (Dec. 10, 2002), at 47 (describing FISA Court of Review's decision as "a landmark decision"), *available at* http://intelligence.senate.gov/shelby.pdf) (last visited Nov. 23, 2004); Dan Eggen, *Broad U.S. Wiretap Powers Upheld; Secret Court Lifts Bar on Terror Suspect Surveillance*, WASH. POST, Nov. 19, 2002, at A1 (reporting civil libertarians' description of Court of Review's decision as a "tremendous setback").

[422] Chemerinsky, *supra* note 6, at 1626.

[423] *See supra* notes 30–31 and accompanying text (summarizing relevant commentary).

[424] *See, e.g., In re* Sealed Case, 310 F.3d at 736–37; 147 CONG. REC. S10597 (daily ed. Oct. 11, 2001) (statement of Sen. Kennedy) (stating that Patriot Act's "significant purpose" amendment "may well make the Foreign Intelligence Surveillance Act unconstitutional under the Fourth Amendment").

[425] *See, e.g.*, 147 CONG. REC. S10558 (daily ed. Oct. 11, 2001) (statement of Sen. Leahy) ("[E]ven the Department [of Justice] concedes that the court's [sic] may impose a constitutional requirement of 'primary purpose' based on the appellate court decisions . . . over the past 20 years."); 147 CONG. REC. S10589 (daily ed. Oct. 11, 2001) (statement of Sen. Edwards) (stating that, while "significant purpose" language was a "substantial improvement" of administration's proposal, the FISA Trial Court "will still need to be careful to enter FISA orders only when the requirements of the Constitution as well as the statute are satisfied").

because it construed the FISA to impose the primary purpose test.[426] By the same token, the FISA Court of Review reached the Fourth Amendment issue only because it did not construe the FISA, of its own force, to impose the primary purpose test.[427] Although the Court of Review did not interpret the FISA to impose the primary purpose test, the court did interpret the FISA to impose some restrictions on the government's use of FISA surveillance for prosecution purposes.[428] If those restrictions rest on flawed statutory interpretation, as this article contends, the Fourth Amendment analysis of the statute would change because the meaning of the statute would change.[429] In short, the Fourth Amendment validity of surveillance under the FISA depends on what the FISA means. Because the Fourth Amendment issue has great importance, so do the statutory issues.[430]

The statutory issues are also timely in light of the government's current need to fight international terrorism and other foreign threats. This point should not be overstated: The Court of Review's decision restricts FISA surveillance much less than did the primary purpose test. Even so, the restrictions operate in two situations. First, the government cannot use FISA surveillance for the sole purpose of getting evidence to prosecute even foreign intelligence crimes such as those arising from international terrorism.[431] Under this restriction, for example, after the 9/11 attacks the government could not have gotten a FISA order solely to gather evidence of Jose Padilla's past

---

[426] *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 614 (Foreign Int. Surv. Ct. 2002) ("The question before the Court . . . raises no constitutional questions that need to be decided.").

[427] *In re* Sealed Case, 310 F.3d at 736 ("Having determined that FISA, as amended, does not oblige the government to demonstrate to the FISA court that its primary purpose in considering electronic surveillance is *not* criminal prosecution, we are obliged to consider whether the statute as amended is consistent with the Fourth Amendment.").

[428] *See supra* notes 391–406 and accompanying text.

[429] *See infra* notes 457–60, 474–520 and accompanying text.

[430] In commenting on a draft of this article, Professors Peter Raven-Hansen and Kim Lane Scheppele incisively observed that the statutory analysis presented here must be informed by consideration of the constitutional issues. This article's focus on the statutory issue does not reflect disagreement with that observation. Indeed, the analysis in this Part of the article discusses at some length the constitutional concerns that influenced various aspects of the original FISA and the Patriot Act provision amending the original FISA's purpose provision. The article's focus on statutory issues reflects my views that (1) in addressing the constitutional issues, the courts and commentators have not paid enough attention to the statutory issues; and (2) careful analysis of the statutory issues may usefully inform analysis of the constitutional issues as well as Congress's consideration of whether the relevant Patriot Act provision, Section 218, should be allowed to sunset. *See infra* notes 436–37 and accompanying text (discussing sunset).

[431] *See* 50 U.S.C. § 1801(c) (2004) (defining "international terrorism").

involvement in those attacks.[432] The government would need a future-oriented objective, as well, such as the prevention of future acts of terrorism. The government usually would have no trouble articulating such an objective, which is why the Court of Review thought this restriction did not pose much of a practical problem.[433] The restriction could, however, complicate the process for getting FISA surveillance for some investigations and lead to litigation over the government's purposes for seeking FISA surveillance orders. Under an additional limitation articulated by the Court of Review, the government cannot use FISA surveillance if its "primary objective" is to prosecute foreign agents for "ordinary crimes" "wholly unrelated" to foreign intelligence.[434] Thus, for example, the government could not use FISA surveillance for the primary (much less the sole) purpose of prosecuting a suspected terrorist of cocaine dealing if the cocaine dealing served only to support the suspect's own drug habit and not to fund her terrorist activity. The government apparently could not do this even if it could show that incapacitating the terrorist advanced foreign intelligence purposes by, for example, thwarting a terrorist attack.[435]

Finally, the statutory rulings will require Congress's attention when it debates reauthorization of the Patriot Act. The provision in the Patriot Act amending the "purpose" provision of the original FISA, as well as the provision in the Patriot Act adding a coordination provision to the FISA, sunsets on December 31, 2005.[436] Congress has the options of (1) doing nothing, i.e., allowing the sunset to occur, in which case the original version of FISA's purpose provision comes back into force; (2) renewing the current Patriot Act provisions that amend the original FISA's purpose provision and that expressly

---

[432] *See* Rumsfeld v. Padilla, 124 S. Ct. 2711, 2715–16 (2004) (describing Padilla's arrest); *see also, e.g.*, Richard B. Schmitt, *Government Says Padilla Plotted High-Rise Attacks; Allegations are released as the Supreme Court prepares to rule on his arrest and detention*, L.A. TIMES, June 2, 2004, at A1 (reporting government's allegation that, "in addition to wanting to plant a 'dirty bomb,' [Padilla] also plotted with Al Qaeda to blow up high-rise apartment buildings in the United States.").

[433] *In re* Sealed Case, 310 F.3d 717, 735 (Foreign Int. Surv. Ct. Rev. 2002).

[434] *Id.* at 736.

[435] *Id.* at 735–36 (rejecting government's argument that "even prosecutions of *non*-foreign intelligence crimes are consistent with a purpose of gaining foreign intelligence information so long as the government's objective is to stop espionage or terrorism by putting an agent of a foreign power in prison," concluding that this argument "transgresses the original FISA").

[436] Patriot Act, § 224(a), 115 Stat. 295 (2001) (providing that, with certain exceptions, provisions including § 218 of the Patriot Act, which amended 50 U.S.C. § 1804(a)(7)(B) to replace "the purpose" with "a significant purpose," expire on Dec. 31, 2005), reproduced as note after 50 U.S.C. § 1802 (2004).

authorize coordination of law enforcement and intelligence activities; or (3) doing something new, i.e., clarifying or substantively changing the statutory law on the permissible purposes of FISA surveillance. Congress should base its choice on "a full and informed debate."[437]

As to the first option, restoration of the original FISA would immediately create a split among the federal courts of appeals. As discussed above, several circuits interpret the original FISA to impose the primary purpose test.[438] The FISA Court of Review rejected that interpretation.[439] This conflict could produce odd results. The Court of Review's decision binds the FISA Trial Court judges who rule on applications for FISA surveillance because the Court of Review can review those judges' decisions.[440] In contrast, the Court of Review's decision does not bind federal district courts in which defendants are prosecuted with FISA-acquired evidence, because those courts' decisions are not subject to review by the Court of Review.[441] Consequently, a FISA judge could approve FISA surveillance for the primary purpose of prosecution, only to have the evidence suppressed if tendered for prosecution in a federal district whose circuit interprets the original FISA to impose the primary purpose test.[442]

The second option, reauthorization of the Patriot Act's amendments to the original FISA, would leave the law unclear and unsettled. The FISA Court of Review has interpreted the FISA, as amended by the Patriot Act, to eliminate the primary purpose test while still putting certain, less stringent restrictions on the government's use of FISA surveillance.[443] As mentioned previously, that interpretation binds only the FISA Trial Court judges.[444] Therefore, courts in which the

---

[437] 9/11 COMM'N REPORT, *supra* note 2, at 394.

[438] *See supra* notes 210–25 and accompanying text.

[439] *See supra* note 427 and accompanying text; *see also* Stephanie Kornblum, Note, *Winning the Battle While Losing the War: Ramifications of the Foreign Intelligence Surveillance Court of Review's First Decision*, 27 SEATTLE U. L. REV. 623, 650 (2003) (observing that FISA Court of Review's interpretation of the original FISA "discredited" circuit precedent construing original FISA to impose "primary purpose" test).

[440] *See In re* Sealed Case, 310 F.3d at 721 (discussing jurisdiction); *supra* notes 75–80 & 341–45 (same).

[441] *See generally* Evan H. Caminker, *Why Must Inferior Courts Obey Superior Court Precedents?*, 46 STAN. L. REV. 817 (1994) (exploring basis for rule that inferior courts must follow precedent of superior courts that can review the inferior courts' decisions).

[442] As Bob Pikowsky observed in commenting on a draft of this article, however, if a later court held that a FISA surveillance order should not have issued, the court still might admit evidence under the good faith exception. *See, e.g.*, Illinois v. Krull, 480 U.S. 340, 349–60 (1987) (using exception to uphold evidence obtained under statute later held unconstitutional).

[443] *See supra* notes 372–409 and accompanying text.

[444] *See supra* notes 440–41 and accompanying text.

government is prosecuting defendants using FISA-acquired evidence remain free to interpret the Patriot Act amendments differently from the FISA Court of Review. They might, for example, interpret the Patriot Act to preserve the primary purpose test.[445] Alternatively, they could (and, as this article argues, should) interpret the Patriot Act to free the government from the restrictions on prosecutorial use of FISA surveillance that were discerned by the FISA Court of Review. Thus, if Congress simply reauthorizes the current Patriot Act provisions, the statutory issues will endure, and their proper resolution is likely to divide the federal courts.[446]

The third option, congressional rethinking, can avoid the potential for conflict and uncertainty in the courts on the meaning of the current statutes, but brings its own uncertainty. Consideration of the third option involves at least two issues: (1) whether existing law needs clarification; and (2) if so, how it should be clarified. The FISA Trial Court interpreted the FISA, even as amended by the Patriot Act, to impose the primary purpose test, but the FISA Court of Review disagreed. Congress could clarify the FISA provisions and, in the process, legislatively ratify either court's interpretation or go in a new direction.

The next two sections of this article offer analysis of these statutory provisions in the hope of shedding light on Congress's options. The analysis is meant not only to inform the debate over the Patriot Act's reauthorization, but also to guide the federal courts. Whatever Congress's decision, the federal courts in current and future prosecutions will be confronted with evidence of crime obtained in FISA surveillance under the current version of the statute. This is inevitable because FISA surveillance has increased sharply after 9/11,[447] as have the number of federal statutes criminalizing various acts of terrorism. The defendants in future prosecutions can challenge

---

[445] *See* 147 CONG. REC. S11003–04 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) (stating that administration's original proposal "raised constitutional concerns," and that, under the compromise version providing for "significant purpose" standard, courts would have to decide "how far" the government could go); Petition of ACLU et al. for a Writ of Certiorari, *In re* Sealed Case, *supra* note 416, at i (framing as one of questions presented: "Does the [Patriot Act] authorize the government to conduct surveillance under the [FISA] even where the government's primary purpose is law enforcement rather than foreign intelligence?").

[446] A bill was introduced in the last Congress that would have repealed the Patriot Act's sunset provision, making all of the Act's provisions permanent. *See* S. 2476, 108th Cong. (2004), reproduced at 150 CONG. REC. S6099 (daily ed. May 21, 2004).

[447] *See* Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Orders 1979-2003*, *available at* http://www.epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Nov. 23, 2004).

the legality of the FISA surveillance on both statutory and constitutional grounds.[448] The statutory issues, therefore, will not go away anytime soon.

B. Statutory Analysis of the Original FISA

As discussed above, the original FISA returns to force if the Patriot Act's amendments to the FISA sunset.[449] In that event, there will be a conflict in the federal courts on the "primary purpose" issue.[450] Several federal circuits interpreted the original FISA to prohibit the government from using foreign intelligence information obtained through FISA surveillance for the "primary purpose" of investigating and prosecuting crime. Those courts relied on the original FISA's purpose provision.[451] The FISA Trial Court adopted the primary purpose test while tying it, not to the purpose provision, but to the FISA provisions on minimization procedures.[452] In contrast, the FISA Court of Review rejected the primary purpose test as an interpretation of any of those statutory provisions.[453] It held that the original FISA "clearly did not preclude or limit the government's use or proposed use of foreign intelligence information . . . in a criminal prosecution."[454] However, it interpreted the term "foreign intelligence information" to exclude "evidence of ordinary crime" unless it is "inextricably intertwined with foreign intelligence crimes."[455]

This section concludes that none of these courts interpreted the original FISA correctly. The original FISA's purpose provision did not impose the primary purpose test, as the test has been articulated by the federal courts.[456] Contrary to the FISA Court of Review's interpretation, however, the original FISA's purpose provision *did* "limit the government's . . . proposed use of foreign intelligence information . . . in a criminal prosecution."[457] Specifically, the original FISA's purpose provision required that the government

---

[448] *See* 50 U.S.C. § 1801(b)–(g).

[449] *See supra* note 436 and accompanying text.

[450] *See supra* notes 438–42 and accompanying text.

[451] *See supra* notes 210–23 and accompanying text.

[452] *See supra* notes 335–40 and accompanying text.

[453] *See supra* notes 350–62 and accompanying text.

[454] *In re* Sealed Case, 310 F.3d 717, 727 (Foreign Int. Surv. Ct. Rev. 2002).

[455] *Id.*at 736 (suggesting, for example, that the government can use FISA surveillance to investigate bank robbery if the bank robberies are undertaken "in order to finance the manufacture of a bomb").

[456] *See infra* notes 469–73 and accompanying text.

[457] *In re* Sealed Case, 310 F.3d at 727.

intend to use the information obtained through FISA surveillance to achieve one or more of five foreign intelligence purposes identified in the FISA's definition of "foreign intelligence information."[458] Thus, the purpose provision prohibited the government from intending to use FISA-acquired information solely for prosecution as an end in itself. That prohibition applied whether or not the anticipated prosecution was for what the Court of Review called "foreign intelligence crimes."[459] By the same token, the original FISA's purpose provision allowed the government to use FISA-acquired information for a prosecution that served a foreign intelligence purpose, even the prosecution of ordinary crimes.[460]

The FISA Trial Court erred in deriving the primary purpose test from the FISA's minimization procedures.[461] There is a connection between the FISA's purpose provision and the FISA's minimization procedures: the purpose provision focuses on the government's *intended* use of information obtained under a proposed FISA surveillance order, whereas the minimization procedures focus on the government's *actual* use of the information so obtained.[462] And just as the purpose provision allows the government to seek a FISA surveillance order for the purpose of getting evidence for a prosecution, the minimization procedures generally allow the information to be actually used for that purpose.[463] The main difference between the scope of intended prosecutions for which a FISA surveillance order can be obtained and the scope of prosecutions that actually may be undertaken is that the latter can include even prosecutions that are not intended to serve a foreign intelligence purpose.[464] In short, the government cannot get a FISA surveillance order for the purpose of pursuing prosecution as an end in itself.[465] But if surveillance under the order nonetheless produces evidence of crime, the government can use that evidence for

---

[458] *See* 50 U.S.C. § 1801(e) (2003) (defining "foreign intelligence information"); *infra* notes 474–82 and accompanying text (explaining interpretation summarized in the text accompanying this note).

[459] *In re* Sealed Case, 310 F.3d at 723 & n.10; *cf. id.* at 736 (apparently amending definition of "foreign intelligence crime" to include "ordinary crimes . . . inextricably intertwined with foreign intelligence crimes").

[460] *Id.* at 735–36.

[461] *See supra* notes 335–40 and accompanying text (describing FISA Trial Court's reliance on FISA provisions on minimization procedures to impose primary purpose test).

[462] *See infra* notes 476–82, 601–04, & 667–69 and accompanying text.

[463] *See infra* notes 596–604 and accompanying text.

[464] *See infra* notes 537 & 604 and accompanying text.

[465] *See infra* notes 537 & 604 and accompanying text.

prosecution regardless of whether the prosecution serves a foreign intelligence purpose.[466] The government does not need to ignore evidence of ordinary crime that falls into its lap.

1. The Purpose Provision of the Original FISA

The original FISA's purpose provision limited the government's intended use of FISA-acquired foreign intelligence information for prosecution purposes. That limit, however, was not accurately captured by the judicially developed primary purpose test. Properly interpreted, the purpose provision allowed the government to undertake FISA surveillance for the primary purpose—even the sole purpose—of getting information for a prosecution of any type of crime, on one condition: the government had to intend the prosecution to serve one or more of five foreign intelligence purposes identified in the FISA. This restriction emerges from both the text and legislative history of the original FISA.

a. Text of the Original FISA's Purpose Provision

i. The Primary Purpose Test's Defective Textual Interpretation

The purpose provision required a high-ranking intelligence official—typically the Director of the FBI (for surveillance targeting U.S. persons)[467]—to certify that "the purpose of the [proposed] surveillance is to obtain foreign intelligence information."[468] The primary purpose case law's reliance on this provision conflicts with the text of the provision in two ways.

First, the text of the purpose provision refers to "the purpose," not "the primary purpose." The statute's use of "the purpose" implies that the sole purpose, not just the primary purpose, be to obtain foreign intelligence information. If that implication is accepted, a requirement that the government certify to the "primary purpose" of the proposed surveillance is more lenient than a requirement that the government certify to "the purpose" of the proposed surveillance. In this sense, the primary purpose precedent read the purpose provision more favorably to the government than it could have (and arguably should have) been read. Perhaps that is why the Department of Justice acquiesced in the

[466] *See infra* note 604 and accompanying text.
[467] *See supra* note 94 and accompanying text.
[468] FISA § 1804(a)(7)(B) (2003).

primary purpose test;[469] it was more generous than a "sole purpose" test.[470] Certainly a strict reading of "the purpose" phrase, in isolation, supported a sole purpose test rather than a primary purpose test.[471]

The primary purpose case law has a second, more fundamental textual problem. The problem lies in the discrepancy between (1) the purpose about which the provision explicitly speaks and (2) the purpose with which the primary purpose test is concerned. The text of the FISA requires the government to have the purpose of obtaining a particular type of information: foreign intelligence information.[472] The text does not, on its face, address what purpose the government must have for wanting that information. Thus, the purpose provision is explicit about the type of information that the government intends to obtain, but not about the government's intended use of that information. The government must certify that the purpose of proposed surveillance is to obtain foreign intelligence information, and not some other type of information. As explained in Part I, there is a difference between having the purpose of obtaining a thing and having the purpose of putting that thing to a particular use.[473] To repeat the analogy proposed in Part I, if I certify to you that I want to borrow $20,000 from you to buy a car, my certification concerns the type of thing I want to obtain, but not how I intend to use that thing. The primary purpose precedent ignores the difference between, on one hand, having the purpose of obtaining a particular type of information and, on the other hand, having the purpose of making a particular use of that information.

ii. The FISA Court of Review's Erroneous Conclusion That the Original FISA's Purpose Provision Did Not Limit the Government's Intended Prosecutorial Use of Foreign Intelligence Information

The FISA Court of Review did not make the same mistake that the primary purpose case law did, but instead erred in a different way. The Court of Review recognized the difference between the purpose

---

[469] *See supra* notes 229–62 and accompanying text (discussing Department's implementation of primary purpose test).

[470] *See* United States v. Truong, 629 F.2d 908, 915 (4th Cir. 1980) (describing defendants' argument that "the 'primarily' test does not go far enough to protect privacy interests" and that "the government should be able to avoid the warrant requirement only when the surveillance is conducted 'solely' for foreign policy reasons.").

[471] *See, e.g.*, Scheppele, *supra* note 3, at 1037 (asserting that original FISA's purpose provision "limited FISA warrants to instances where the government could assert . . . that the surveillance was undertaken exclusively for national security purposes.").

[472] *See* FISA § 1804(a)(7)(B) (2003).

[473] *See supra* notes 132–36 and accompanying text.

of obtaining a particular type of information and the intended use of the information, saying that the FISA apparently required a judge reviewing a government application for proposed surveillance to determine "whether the information sought is actually foreign intelligence information, not the government's proposed use of that information."[474] Because FISA's purpose provision explicitly addressed the purpose of obtaining a particular type of information and did not explicitly address the government's intended use of that information, the Court of Review concluded that the FISA "clearly did not preclude or limit the government's use or proposed use of foreign intelligence information . . . in a criminal prosecution."[475] However, the court went too far in concluding that the FISA puts no limit on the government's intended use of foreign intelligence information for prosecutions.

As explained in Part I, although the original FISA's purpose provision does not expressly address the government's intended use of FISA-acquired foreign intelligence information, the provision does so implicitly.[476] That is because of the manner in which FISA defines the term "foreign intelligence information," as it concerns U.S. persons. The FISA defines "foreign intelligence information" instrumentally, i.e., by its usefulness to achieving one or more of five purposes.[477] It is information:

> (1) . . . necessary to, the ability of the United States to protect against—
>
> (A) [1] actual or potential attack or other grave hostile acts of a foreign power;
>
> (B) [2] sabotage or international terrorism by a foreign power or an agent of a foreign power;
>
> (C) [3] clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) . . . necessary to—

---

[474] *In re* Sealed Case, 310 F.3d 717, 724 (Foreign Int. Surv. Ct. Rev. 2002).

[475] *Id.* at 727.

[476] *See supra* notes 136–38 and accompanying text.

[477] *See* S. REP. NO. 95-604, at 31 (1977) (reporting that definition of foreign intelligence information "set out standards establishing a nexus between the information sought and the desired end"; for U.S. persons, government must demonstrate "a significant degree of need" for surveillance); H.R. REP. NO. 95-1283, pt. 1, at 47 (1978) ("Where the term 'necessary' is used, the committee intends to require . . . a showing that the information is both important and required. The use of this standard is intended to mandate that a significant need be demonstrated by those seeking the surveillance.").

(A) [4] the national defense or the security of the United States; or

(B) [5] the conduct of the foreign affairs of the United States.[478]

When the purpose provision is read in light of this definition, it requires the government to certify that the purpose of proposed surveillance is to obtain information that is necessary to the government's achievement of one or more of the five foreign intelligence purposes identified in the definition. In effect, then, the purpose provision requires the government to certify two things: (1) the government's purpose is to obtain particular information; and (2) that information is necessary to the government's achievement of a statutorily specified foreign intelligence purpose.

So understood, the original FISA's purpose provision should be read to limit the government's intended use of foreign intelligence sought under a FISA surveillance order. To again reprise the reasoning by analogy laid out in Part I: if I certify to you that (1) "the purpose" of my borrowing $20,000 from you is to buy a car; and (2) the car is "necessary to" my ability to get to work, I am strongly implying that I intend to use the car to get to work. Furthermore, you probably required me to make those certifications because you wanted to require me to have the intention of using the car to get to work. Likewise, if the government certifies that (1) "the purpose" of proposed FISA surveillance is to obtain information X; and (2) information X is "necessary to" the government's ability, say, to protect against international terrorism by a foreign power, the government is strongly implying that it intends to use information X to protect against such international terrorism. Furthermore, by requiring those certifications, Congress probably meant to require the government to have that intended use in mind when applying for a surveillance order. In short, the text of the original FISA's purpose provision, read in light of the FISA's definition of "foreign intelligence information," requires the government to intend to use foreign intelligence information sought under a proposed surveillance order for one or more of the five foreign intelligence purposes specified in the definition of "foreign intelligence information."

This interpretation of the original FISA's purpose provision gets support from the FISA's requirements about the process of certification. FISA requires the purpose certification to be made by a high-ranking intelligence official, i.e., "the Assistant to the President

[478] 50 U.S.C. § 1801(e) (2003).

for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate."[479] Further, that official must designate the type of foreign intelligence information being sought according to the categories identified in the definition of foreign intelligence information.[480] In addition, he or she must state the basis for the certification that the information sought is the type designated.[481] Having imposed those requirements, Congress presumably would have considered it dishonest for a high-ranking intelligence official to certify that "the purpose" of proposed surveillance was to obtain designated information that was "necessary to" achieving a foreign intelligence purpose, if the government had no intention of using the information for that purpose.

The FISA Court of Review therefore erred in holding that the purpose provision "clearly did not preclude or limit the government's . . . proposed use of foreign intelligence information . . . in a prosecution."[482] The government could not seek a FISA surveillance order if its proposed purpose was solely to pursue prosecution as an end in itself. If the government sought a FISA surveillance order for the sole purpose of getting evidence for a prosecution, the government had to intend that the anticipated prosecution be instrumental to a statutorily specified foreign intelligence goal.

iii. The Requirement that Achievement of a Foreign Intelligence Purpose be the Primary Purpose for Seeking a FISA Surveillance Order

The analysis so far interprets the original FISA as requiring the government, when seeking a FISA surveillance order, to intend to use the information sought under the order for one or more of the five foreign intelligence purposes identified in the definition of foreign intelligence information. The FISA can also be read to impose a further requirement: that the government's "primary purpose" for seeking the order be to achieve a foreign intelligence purpose. This reading, however, does not vindicate the judicial "primary purpose"

---

[479] *Id.* § 1804(a)(7).
[480] *Id.* § 1804(a)(7)(D).
[481] *Id.* § 1804(a)(7)(E)(i).
[482] *In re* Sealed Case, 310 F.3d 717, 727 (Foreign Int. Surv. Ct. Rev. 2002).

test, because that test incorrectly assumes incompatibility between foreign intelligence purposes and law enforcement purposes.

In general, a person can intend to obtain a thing that is necessary to achieve some purpose without having the achievement of that purpose be his or her primary motivation for obtaining the thing.[483] To repeat the analogy proposed in Part I: Suppose a teenager certifies to her parent that (1) "the purpose" of her borrowing money from the parent is to buy a car; and (2) the car is "necessary to" her fulfillment of work and school obligations. By making these certifications, the teenager implies that she intends to use the car to get to work. That intended use, however, may not be her primary motivation for seeking the loan or getting the car.[484]

Likewise, you might first think, the government can satisfy the original FISA's purpose provision if it intends to use the foreign intelligence information sought under a proposed surveillance order for a foreign intelligence purpose, even if that is not the government's primary purpose for seeking the information—even if, more specifically, the government's primary purpose is simply to put a criminal in prison, regardless of the foreign intelligence benefits of doing so. As long as the government intends the prosecution to advance a foreign intelligence purpose, it does not matter that this intended effect of the prosecution is not the government's primary motivation for the surveillance.[485]

This reasoning, however, ignores the FISA provisions specifying who has to make the required certification about the purpose of proposed surveillance and how the certification must be made. FISA requires the purpose certification to be made by an official "designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate."[486] Thus,

---

[483] *See supra* notes 132–36 and accompanying text (elaborating on this point).

[484] *See supra* section I.B.3.a.

[485] Professor Banks argues that, under both the original FISA and FISA as amended by the Patriot Act, "the FISA mechanisms are available *only* when the purpose (or, after enactment of the Patriot Act, a 'significant purpose') of the surveillance . . . is to gather foreign intelligence, even though the information collected may include evidence of a crime and that such evidence could be used later in a criminal prosecution." Banks, *supra* note 30, at 1178. As I understand this argument, it does not accept the analysis offered in this article, which asserts that having a purpose of gathering foreign intelligence information is equivalent to having a purpose of getting evidence for a prosecution if the prosecution is thought necessary to serve one or more of the foreign intelligence purposes identified in the FISA's definition of "foreign intelligence information." Thus, the issue is joined.

[486] 50 U.S.C. § 1804(a)(7) (2003).

someone whose job is to protect national security or defense must certify that the purpose of proposed surveillance is to obtain information that (if it concerns a U.S. person) is "necessary" to protect the country from one or more of three kinds of foreign threats to national security,[487] the national defense,[488] or to the conduct of foreign affairs.[489] Congress presumably required such a person to make the certification to ensure that the primary purpose of the proposed surveillance was to achieve one of these foreign intelligence goals.[490] To use the analogy described in Part I, suppose the director of information technology for a large company certifies to the company's chief financial officer that (1) the director needs $2 million dollars to upgrade company computers; and (2) the upgrade is necessary for the company to protect the company computer system from viruses and computer hackers. The chief financial officer can reasonably infer that the director's primary purpose for seeking the money is to protect the company's computer system from the specified outside threats. The connection between the certifier's official responsibilities and the purpose to be achieved by the thing sought supports the inference that the primary purpose of obtaining the thing is to achieve that purpose.

Thus, the FISA's purpose provision can be read to require the government to use FISA surveillance for the primary purpose of achieving one or more of the five foreign intelligence purposes specified in FISA's definition of "foreign intelligence information." This reading does not resolve whether the government can use FISA surveillance to get evidence for a prosecution if its primary purpose for doing so is its determination that the prosecution will advance a foreign intelligence purpose—for example, by preventing an attack by

---

[487] *See id.* § 1801(e)(1) (defining "foreign intelligence information" to include information that, if it concerns a U.S. person, is "necessary to . . . the ability of the United States to protect against" three kinds of foreign threats).

[488] *See id.* § 1801(e)(2)(A) (defining "foreign intelligence information" to include information that, if it concerns a U.S. person, is "necessary to . . . the national defense or the security of the United States").

[489] *See id.* § 1801(e)(2)(B) (defining "foreign intelligence information" to include information that, if it concerns a U.S. person, is "necessary to . . . the conduct of the foreign affairs of the United States").

[490] This conclusion is reinforced by two additional requirements in FISA. FISA requires the certifier to designate which of the five foreign intelligence purposes identified in the definition of foreign intelligence information will be served by the information sought. *See id.* § 1804(a)(7)(D) (requiring certification "that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title [which defines "foreign intelligence information]"). Beyond that, FISA requires the person to include "a statement of the basis for the certification that . . . the information sought is the type of foreign intelligence information designated." *Id.* § 1804(a)(7)(E)(i).

international terrorists inside the United States. Thus, while FISA may be read to impose a "primary purpose" requirement, that requirement, as elucidated so far, differs in a critical way from the judicially created "primary purpose" test discussed above. The "judicial primary purpose test" (as it will be referred to hereafter) assumes incompatibility between foreign intelligence purposes and law enforcement purposes. Thus, it implicitly rejects the notion that the government can use law enforcement means to further a foreign intelligence purpose. This rejection can be seen in both the case law that derives the primary purpose test from the original FISA's purpose provision and the FISA Trial Court's decision, which derived the primary purpose test from the FISA's provisions on minimization procedures.[491] This leads to an examination of whether FISA allows the government to seek FISA surveillance for prosecutions intended to advance a foreign intelligence purpose.

iv. The Permissibility, Under the Original FISA, of the Government's Using FISA Surveillance for the Primary (or Even the Sole) Purpose of Investigating and Prosecuting Crime of any Type When the Government Intended the Prosecution to Serve a Foreign Intelligence Purpose

Two questions remain: Can arrest and prosecution serve a foreign intelligence purpose? And if so, did Congress in the original FISA accept that fact, thereby authorizing the government to get a FISA surveillance order for the purpose of prosecutions that served a foreign intelligence purpose? These questions have particular salience because, before In re *Sealed Case*, the government had never argued that prosecutions can serve foreign intelligence purposes.[492] The argument's recent vintage raises doubts about the validity of the argument. It seems useful to examine those doubts from two

---

[491] United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984) (upholding FISA surveillance on the ground that its purpose "was to secure foreign intelligence information and was not . . . directed towards criminal investigation or . . . criminal prosecution.'") (quoting United States v. Megahey, 553 F. Supp. 1180, 1190 (E.D.N.Y. 1982)); *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 623 (Foreign Int. Surv. Ct. 2002) (holding that Attorney General's March 2002 information sharing procedures were invalid because, and to the extent that, they were "designed to enhance the acquisition, retention, and dissemination of *evidence for law enforcement purposes*, *instead* of being consistent with the need of the United States to 'obtain, produce, and disseminate *foreign intelligence information*.'") (quoting 50 U.S.C. §§ 1801(h), 1821(4)) (emphasis added by the FISA Trial Court).

[492] *See* Oral Argument Transcript at 51–62, *In re* Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002) (No. 02-001).

perspectives: first, whether, as a factual matter, a prosecution based on FISA-acquired evidence can advance a foreign intelligence purpose; and, second, whether even if that theory is true, it should inform the interpretation of the original FISA.

The first question has become easy to answer, at least since the United States began responding to "the new terrorism."[493] Certainly, prosecution can serve foreign intelligence purposes by protecting the country from foreign threats.[494] The foreign intelligence purposes identified in the FISA's definition of "foreign intelligence information" include three protective purposes: protection against

> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.[495]

Each threat arises from the conduct of foreign powers or their agents. Prosecutors cannot ordinarily reach foreign powers, but they often can indict foreign agents and bring them to trial. The arrest and jailing of a foreign agent can disable that agent from contributing to the foreign threat.[496] The prospect of prosecution can convince the agent to assist government investigators by providing information or assisting the United States in other ways.[497] Actual prosecution, if

---

[493] 9/11 COMM'N REPORT, *supra* note 2, at 47 (chapter entitled "The Foundation of the New Terrorism").

[494] *See, e.g.*, *id.*, at 72 (describing arrests that "disrupt[ed]" international terrorists' "landmarks plot" to bomb New York landmarks including Holland and Lincoln tunnels); *see also* 2003 Attorney General's Guidelines for FBI National Security Investigations, *supra* note 316, at 2 (including "arresting and prosecuting the perpetrators" among "a variety of measures to deal with threats to the national security"); Scheppele, *supra* note 3, at 1024–25 (describing Clinton Administration's antiterrorism efforts as reflecting the belief that "the ordinary criminal justice system was an effective tool" against terrorism).

[495] 50 U.S.C. § 1801(e)(1) (2003).

[496] Two recent examples are the arrest and prosecution of Ahmed Ressam, who was detained at the Canadian border carrying explosives that he intended to use in the United States at the millennium, and Richard Reid, who was detained in December 2001 after he attempted, while on a flight from Paris to Miami, to ignite a shoe bomb. 9/11 COMM'N REPORT, *supra* note 2, at 176–79 (describing Ressam's plot and its failure); *Joint Inquiry*, *supra* note 3, at 126 (pagination of unclassified version) (summarizing Reid's plot and its failure).

[497] *See, e.g.*, H.R. REP. 95-1283, pt. 1, at 43–44 (1978) ("One might wonder why the Government would not immediately arrest [known international terrorists]. In some cases . . . it may be more fruitful in terms of combating international terrorism to identify otherwise unknown terrorists here, their international support structure, and the location of their weapons or explosives."); *Senate Intelligence Hearing on Patriot Act*, *supra* note

successful, can take the agent off the street for a long time (or permanently).[498] In addition, news of the arrest and prosecution can derail the threat in which the agent is involved and deter other threats.[499]

Furthermore, this potential for prosecution to serve a protective function exists whether or not the prosecution is for a crime arising out of the threatening foreign activity or, instead, an unrelated crime such as rape of a domestic partner.[500] Thus, the FISA Court of Review erred in concluding that the government cannot use FISA surveillance to prosecute "non-foreign intelligence crimes."[501] Significantly, the FISA does not use the terms "foreign intelligence crimes" and "non-foreign intelligence crimes." Instead, the FISA authorizes the government to use FISA to obtain any information that is "necessary to" one of five purposes, three of which concern protecting the United States from specified foreign threats. If the government can legitimately certify that it needs to get evidence of crime by a foreign agent to take that agent off the street and thereby thwart a foreign threat, that evidence is "foreign intelligence information" regardless of the type of crime that it concerns. The Court of Review accepted this reasoning only up to a point. The court

---

291, at 33 (testimony of David Kris, Associate Deputy Attorney General, United States Department of Justice) (describing argument that "prosecution of spies and terrorists is just one more counterintelligence tool . . . [and] [b]y surveilling them we can recruit them, double them [i.e., turn them into a double agent], we can cut them off from access to classified information, we can PNG [i.e., throw them out of the country as a "persona non grata"], or possibly prosecute them."); Oral Argument Transcript at 7–9, *In re* Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002) (argument of Theodore Olson, Solicitor General of United States) (describing ways that government can use FISA-acquired information, including prosecution).

[498] For example, Ahmed Ressam, convicted of smuggling explosives from Canada into the United States right before the millennium (*see supra* note 496), faces up to 130 years of imprisonment, but, as of this writing, his sentencing has been delayed to determine whether the potential sentence should be reduced because of his cooperation with investigators. *See, e.g.*, Wendy Kaufman, *Convicted terrorist Ahmed Ressam could receive lighter sentence after cooperating with the government in other terrorist cases*, National Pub. Radio, Mar. 27, 2002, *available at* 2002 WL 3187574. Richard Reid, the convicted "shoe bomber" (*see supra* note 496), got life in prison. *See* John Berman, *Richard Reid Sentenced Shoe Bomber Gets in Confrontation with Judge*, ABC News: World News This Morning (Jan. 31, 2003), *available at* 2003 WL 5025736.

[499] *See, e.g.*, 9/11 COMM'N REPORT, *supra* note 2, at 272 (observing that if government had detained two of the 9/11 hijackers that various officials were in fact trying to track down before 9/11, "[t]he simple fact of their detention could have derailed the plan").

[500] *See infra* notes 682–684 and accompanying text (elaborating on the point that prosecution of foreign agents for "ordinary crime" can serve foreign intelligence purposes).

[501] *In re* Sealed Case, 310 F.3d 717, 735–36 (Foreign Int. Surv. Ct. Rev. 2002). By "non-foreign intelligence crimes," the court meant "ordinary crimes" such as bank robbery, which, at the time of their commission, are "wholly unrelated" to "foreign intelligence crimes."; *see also id.* at 723 & n.10.

recognized that "arresting and prosecuting [foreign agents] may well be the best technique to prevent them from successfully continuing their terrorist or espionage activity."[502] The court nonetheless thought it would "transgress[] the original FISA" if the government used FISA surveillance to prosecute a foreign agent for a "non-foreign intelligence crime."[503] To the contrary—if one accepts that the arrest and prosecution of foreign agents can serve the protective foreign intelligence purposes identified in the FISA—the Court of Review's decision transgressed the original FISA by restricting the government's ability to get foreign intelligence information based on a distinction, i.e., between "foreign intelligence crimes" and "non-foreign intelligence crimes," that the FISA does not contain.[504]

Assuming that arrest and prosecution can serve a protective foreign intelligence purpose, the question remains whether this potential protective function of prosecution can inform interpretation of the original FISA, so as to allow the government to seek a FISA surveillance order for the purpose of prosecuting crimes that serve a foreign intelligence purpose. This question is easy to answer affirmatively if one accepts the legislative history specifically endorsing this theory. Some of the relevant history is reproduced in the FISA Court of Review's opinion.[505] Additional relevant history is discussed in the next subsection of this article.[506] The same answer emerges from the text of the original FISA, which shows that ordinarily it is up to the executive branch to decide whether a prosecution with FISA-acquired information would advance a foreign intelligence purpose. The FISA required a high-ranking intelligence official to certify that he or she "(A) deems the information sought to be foreign intelligence information; [and] (B) that the purpose of the surveillance is to obtain foreign intelligence information."[507] The official could "deem" the information sought to be foreign intelligence information if she determined it was necessary to a prosecution that would protect the country against an act of international terrorism. The FISA judge reviewing the application in

---

[502] Id. at 724.

[503] Id. at 735–36.

[504] The Court of Review carved out an exception for "non-foreign intelligence crimes" partly because of its understanding of legislative history. *See In re* Sealed Case, 310 F.3d at 736. For the relevant legislative history, see *infra* notes 554–57 & 571–76 and accompanying text.

[505] *See supra* notes 354–60 and accompanying text.

[506] *See infra* notes 559–60 and accompanying text.

[507] 50 U.S.C. § 1804(a)(7)(A), (B) (2003).

which these certifications were made would apply a "clearly erroneous" standard of review, if the target of the proposed surveillance was a U.S. person.[508] That standard gives deference to the official's certification that the intended prosecution would serve a foreign intelligence purpose. Given this standard of judicial review, the nature of the certifications, and the position of the official who makes the certifications, it does not matter that the government has only recently articulated the protective foreign intelligence purposes served by prosecution in litigation over the "primary purpose" test, especially considering the government's long acquiescence in the primary purpose test.[509] All that matters is that in a particular application for proposed surveillance the government can establish, in a way that is not clearly erroneous, its purpose to obtain "foreign intelligence information."

The legislative history discussed below suggests that, when Congress enacted the original FISA, the executive branch seldom used prosecution to protect against foreign threats.[510] This in turn suggests that when the government did prosecute crimes such as espionage and sabotage, it was pursuing prosecution as an end in itself, and not because of its instrumental value for achieving foreign intelligence purposes.[511] The analysis of FISA proposed in this article prohibits FISA from being used for such noninstrumental prosecutions. Thus, today, as in 1978, if the government wants to conduct surveillance for the primary purpose of getting evidence for a prosecution that is not intended to serve foreign intelligence purposes, it must meet the requirements of Title III.[512]

---

[508] *Id.* § 1805(a)(5).

[509] *See supra* notes 229–86 and accompanying text.

[510] *See infra* notes 542–53 and accompanying text; *see also* E-Mail from William F. Funk, Professor of Law, Lewis & Clark Law School, to Richard H. Seamon (Oct. 8, 2004) (on file with author) (explaining that because major acts of international terrorism had not been directed at the United States when FISA was enacted, it was "unanticipated" that government would seek to use foreign intelligence surveillance techniques for law enforcement purposes).

[511] *See Church Committee Hearing on the FBI*, *supra* note 64, at 347 (hearing exhibit entitled "FBI Functional Organization Chart," reflecting that FBI had an "Intelligence Division" separate from its "General Investigative Division" and "Special Investigative Division"); *id.* at 348 (hearing exhibit reflecting that a "counterintelligence" unit exists within the Intelligence Division); *see also id.* at 8 (testimony of Frederick A.O. Schwarz, Chief Counsel to Committee) (explaining that counterintelligence unit "involves primarily the FBI's efforts to deal with the activities of unfriendly foreign governments in the United States, largely counterespionage").

[512] *See* Pub. L. No. 90-351, Title III, § 802, 82 Stat. 216 (original provision of Title III authorizing electronic surveillance for evidence of espionage and sabotage) (current version codified at 18 U.S.C. § 2516(1)(a)); *see also* 124 CONG. REC. 28, 124 (1978) (statement of Rep. Rudd) (stating that, under then existing practice, if FBI detected

Nonetheless, the government is not estopped by the former infrequency with which it used prosecution for foreign intelligence purposes. The variety and nature of foreign threats has changed since Congress enacted the original FISA. In particular, the United States faces a much greater threat of terrorist attacks inside the United States today than it faced in 1978.[513] FISA does not restrict how information acquired through FISA surveillance is used to achieve foreign intelligence purposes. Rather, FISA simply requires that the information, if it concerns a U.S. person, be "necessary" for those purposes. Newly discovered means of protection are not prohibited on the grounds of novelty alone. Thus, for example, FISA allows the government to use technology invented since 1978 to store and analyze the information obtained through FISA surveillance. Furthermore, the advent of that technology may cause certain information to be "necessary" to a foreign intelligence purpose today even if that same information would not have been necessary in 1978.[514] Similarly, the FISA allows the government to use prosecution to achieve foreign intelligence purposes even if the government rarely so used it in the past.[515] The judicial primary

---

criminal activity while conducting warrantless electronic surveillance for foreign intelligence information, "a warrant would be sought for further authority to collect evidence by electronic surveillance"); E-mail from William F. Funk, Professor of Law, Lewis & Clark Law School, to Richard H. Seamon, Associate Professor of Law, University of Idaho College of Law (Oct. 2, 2004) (on file with author) (stating that Justice Department personnel involved in drafting predecessor bill, S. 3197, 94th Cong. (1976), "never imagined that the government would use FISA to obtain a surveillance for the primary purpose of prosecuting someone" but instead believed that, if prosecution was the primary purpose, "then Title III was required"); *cf.* Exec. Order No. 12,036, 3 C.F.R. 125 (1978) (requiring Attorney General to approve and find that target of proposed electronic surveillance is an agent of a foreign power whenever electronic surveillance is such that "a warrant would be required if undertaken for law enforcement rather than intelligence purposes").

[513] *See, e.g.*, 9/11 COMM'N REPORT, *supra* note 2, at 96–107 (describing history of terrorist attacks on U.S. interests beginning in 1970s, almost all of which, until the 1990s, occurred outside the United States); *see also* E-Mail from W. Funk to R. Seamon, *supra* note 510 (explaining that, when FISA was enacted, all of the major international terrorism attacks had been directed at countries other than the United States, and that this contributed to "the lack of foresight of the need to use criminal prosecution to stop international terrorists in the United States").

[514] For example, highly detailed map coordinates for a terrorist training camp may be necessary to launching a sophisticated missile against the camp, even though such detailed coordinates would have had little usefulness in 1978.

[515] A history of government non-use of FISA surveillance for prosecutorial purposes would not be entitled to *Chevron* deference, because courts do not grant *Chevron* deference to the Justice Department's interpretation of criminal statutes. *See, e.g.*, Dan M. Kahan, *Is* Chevron *Relevant to Federal Criminal Law?*, 110 HARV. L. REV. 469, 490 n.115 (1996) (citing cases). Professor Kahan, however, argues that they should. *Id.* at 489–506. His argument would not seem to apply here because the Department has never, based on deliberation, officially articulated the view that it cannot use FISA surveillance to get

purpose test errs in denying the government's power to do so under the original FISA.[516]

v. Summary of Textual Analysis of the Original FISA's Purpose Provision

The original FISA's purpose provision allows the government to obtain a FISA surveillance order for the sole or primary purpose of getting evidence for a prosecution of any crime, as long as the government intends the prosecution to serve one or more of the five foreign intelligence purposes identified in the FISA's definition of "foreign intelligence information." Prosecution (and the events leading up to it, including arrest, custodial interrogation, charge and plea bargaining, etc.)[517] can serve the protective foreign intelligence purposes identified in the FISA's definition of "foreign intelligence information."[518] Thus, the primary purpose case law is wrong in interpreting the purpose provision to prohibit the government from getting a FISA surveillance order if its primary purpose is to get evidence for a prosecution. On the other hand, the FISA Court of Review was also wrong in interpreting the provision not to limit the government's intended use of FISA-acquired foreign intelligence information for prosecution.[519] The Court of Review erred, as well, in construing the FISA to bar the government from using FISA surveillance to prosecute "non-foreign intelligence crimes."[520]

---

evidence for a prosecution that would serve a foreign intelligence purpose. *See id.* at 493-504.

[516] This flaw in the judicial primary purpose test will make a big difference if the Patriot Act's "significant purpose" amendment sunsets, and the original FISA's purpose provision comes back into force. In that event, the judicial primary purpose test will (in some circuits) bar the government from using FISA surveillance for the primary purpose of getting evidence for a prosecution. In contrast, the analysis proposed in this article would allow such use as long as the government intended the anticipated prosecution to serve a foreign intelligence purpose.

[517] *See* H.R. CONF. REP. NO. 95-1720, at 23 (1978) (defining "law enforcement purposes" to include "arrest, prosecution, and other law enforcement measures taken for the purpose of preventing the crime").

[518] 50 U.S.C. § 1801(e)(1).

[519] *In re* Sealed Case, 310 F.3d 717, 727 (Foreign Int. Surv. Ct. Rev. 2002) (concluding that the original FISA "clearly did *not* limit the government's . . . proposed use of foreign intelligence information . . . in a criminal prosecution"). Rather than interpreting the original FISA to restrict the government's intended use of FISA-acquired information, the Court of Review interpreted the original FISA to impose a restriction based on whether the government actually used FISA-acquired information to prosecute a "foreign intelligence crime" or a "non-foreign intelligence crime." *See id.* at 731, 734–36.

[520] *Id.* at 735–36.

b. Legislative History of the Original FISA's Purpose Provision

The textual analysis above interprets the original FISA's purpose provision to put two kinds of limits on the government's purpose for seeking a FISA surveillance order, but not to impose the judicial primary purpose test. First, "the purpose" of the proposed surveillance must be to obtain "foreign intelligence information," and not some other type of information.[521] Second, the government must intend to use that information for one or more of the five foreign intelligence purposes identified in the definition of "foreign intelligence information."[522] Textual analysis adds that the use of the information for a foreign intelligence purpose probably must be the government's primary purpose for seeking the surveillance order. But this "primary purpose" requirement, unlike the judicial primary purpose test, recognizes that the prosecutorial use of FISA-acquired information can be necessary to achieving a foreign intelligence purpose.[523] Finally, the textual analysis finds that prosecution of any type of crime by a foreign agent—not just "foreign intelligence crimes"[524]—can potentially advance a foreign intelligence purpose by protecting the country from a foreign threat.[525]

Each aspect of the textual analysis finds support in the legislative history, though some of the history is equivocal. Specifically, the legislative history confirms that the original FISA's purpose provision was meant to restrict both (1) the type of information that the government could use FISA surveillance to obtain as well as (2) the purposes for which it could obtain the information. Some legislative history on the second restriction supports the judicial primary purpose test as the specific restriction that Congress intended to impose. Nonetheless, the legislative history is better understood as merely reflecting that the government cannot use FISA surveillance to pursue prosecution as an end in itself. That understanding gets strong support from the legislative history recognizing that the use of foreign intelligence information for prosecution can further foreign intelligence purposes by protecting the country from foreign threats. Each aspect of the legislative history is discussed below.

---

[521] *See supra* notes 472–73 and accompanying text.

[522] *See supra* notes 476–82 and accompanying text.

[523] *See supra* notes 483–99 and accompanying text.

[524] *In re* Sealed Case, 310 F.3d at 723 & n.10 (defining "foreign intelligence crimes"). *But cf. id.* at 736 (apparently redefining "foreign intelligence crimes" to include "ordinary crimes . . . inextricably intertwined with foreign intelligence crimes").

[525] *See supra* notes 500–04 and accompanying text.

i. Legislative History Showing that the FISA Purpose Provision Limits the Type of Information That can be Sought as Well as the Intended Use of That Information

The legislative history confirms the two types of limits that Congress intended the FISA's purpose provision to impose. The House report on the bill that became the FISA said that the purpose provision served to

> prevent the practice of targeting, for example, a foreign power for electronic surveillance when the true purpose of the surveillance is to gather information about an individual for other than foreign intelligence purposes. It is also designed to make explicit that the sole purpose of such surveillance is to secure "foreign intelligence information," as defined, and not to obtain some other type of information.[526]

This passage identifies two functions of the purpose provision: (1) preventing the acquisition of information "for other than foreign intelligence purposes"; and (2) preventing the acquisition of information other than foreign intelligence information. The first function concerns the intended use of foreign intelligence information; the second concerns the type of information that can be obtained.

Significantly, the FISA Court of Review quoted the very same passage from the House report that is reproduced above, but referred only to the function described in the passage's second sentence—namely, the purpose provision's restriction on the type of information that the government can seek through FISA surveillance.[527] In introducing the passage, the court said it showed Congress's "concern[] about the government's use of FISA surveillance to obtain information not truly intertwined with the government's efforts to protect against threats from foreign powers."[528] The court makes the same point later when it says, "Congress intended section 1804(a)(7)(B) [the purpose provision] to prevent the government from targeting a foreign agent when its 'true purpose' was to gain non-foreign intelligence information, such as evidence of ordinary crimes or scandals."[529] Thus, the Court of Review recognized that the purpose provision limited the type of information that the government

---

[526] *In re* Sealed Case, 310 F.3d at 725 (quoting H.R. REP. NO. 95-1283, pt. 1, at 76 (1978)).

[527] *See id.* at 725, 736, discussed *supra* notes 367–71 and accompanying text.

[528] *Id.* at 725 (emphasis added).

[529] *Id.* at 736 (emphasis added).

can use FISA surveillance to obtain; however, the court did not acknowledge that the purpose provision also restricted the government's intended use even of foreign intelligence information. To the contrary, the court interpreted the original FISA as "not preclud[ing] or limit[ing] the government's proposed use of foreign intelligence information . . . in a prosecution."[530] This interpretation ignores the first sentence of the passage quoted above, which evinces congressional intent to limit the purposes for which the government can seek foreign intelligence information, as well as the type of information that could be sought.

The legislative history shows why Congress wanted to limit both the type and the intended uses of information obtained through FISA surveillance. Specifically, Congress wanted to prevent the abusive surveillance practices documented in the Church Committee reports.[531] As discussed in Part I, the abusive practices concerned both the type of information that government officials collected and the uses to which the officials put that information.[532] The information included "personal" and "political" information that was "unrelated to any legitimate government interest."[533] The uses included embarrassing, harassing, and undermining various officials' political opponents and critics of the government.[534] The legislative history of the FISA reflected Congress's awareness that even foreign intelligence information can be misused.[535] Accordingly, as argued

---

[530] *Id.* at 727; *see also id.* at 724 (stating that language of FISA "suggests that" the FISA court reviewing an application for FISA surveillance should decide only "whether the information sought is actually foreign intelligence information—not the government's proposed use of that information").

[531] *See supra* notes 60–66 and accompanying text.

[532] *See supra* notes 62–65 and accompanying text.

[533] *See, e.g.*, S. REP. NO. 95-604, at 8 (1978) (quoting Church Committee report).

[534] *Senate Intelligence Hearing on FISA*, *supra* note 42, at 278–79, 296–97 (reproducing portions of Church Committee report summarizing instances in which Pres. Kennedy used wiretap information for political purposes).

[535] *See, e.g.*, *Senate Intelligence Hearing on FISA*, *supra* note 42, at 133 (prepared statement of Steven Rosenfeld, Comm. on Fed. Legislation, Ass'n of Bar of NYC) ("Misuse of intelligence information has been an abuse at least as serious and as far reaching as those involved in the gathering of such information. Legislation which regulates the intelligence-gathering process, but is practically silent on the permissible uses of intelligence, accomplishes only half the job."); *id.* at 199 (statement of Sen. Bayh) (stating, in discussion of committee amendment to provision requiring compliance with minimization procedures, that compliance with use restrictions is "one of the most important aspects of this bill. You talk about how you collect, what you collect, and against whom do you collect, but the really critical question is what do you do with that information when you get it."); *see also* H.R. CONF. REP. NO. 95-1720, at 23 (1978) (expressing conferees' judgment that "the standard for dissemination should be higher than for acquisition and retention"); Philip A. Lacovara, *Presidential Power to Gather Intelligence: The Tension Between Article II and Amendment IV*, 40 LAW & CONTEMP.

above, the original FISA's purpose provision prevents the government from seeking even information that fits the definition of foreign intelligence information if the government's "true purpose" is something "other than foreign intelligence purposes."[536] Thus, the government could seek information solely to prosecute a crime only if the government intended the anticipated prosecution to serve a foreign intelligence purpose. By the same token, seeking information for prosecution as an end in itself would be just as improper as seeking the information for the purpose of, say, squelching political dissent.[537]

ii. Legislative History Seemingly Supporting the "Primary Purpose" Test

The legislative history discussed above shows that Congress designed the original FISA's purpose provision to restrict not only the type of information that the government could use FISA surveillance to obtain but also the purpose for which the government could seek that information. Of course, legislative history showing that the purpose provision restricted the purposes for which the government could use FISA surveillance is consistent with the judicial primary

---

PROBS. 106, 106 (Summer 1976) ("The collection of intelligence has no moral dimension as such. It takes on its coloration from the purposes for which the process is pursued, the manner in which the collection proceeds, and the uses to which the information is put.").

[536] *In re* Sealed Case, 310 F.3d 717, 725 (Foreign Int. Surv. Ct. Rev. 2002) (quoting H.R. REP. NO. 95-1283, at 76 (1978)).

[537] *See supra* notes 64–65 and accompanying text. As discussed *supra* in notes 527–30, the FISA Court of Review recognized only one of the two functions of the original FISA's purpose provision. Specifically, the court recognized only that it served to limit the *type* of information that the government could seek; the government could not seek "non-foreign intelligence information." *In re* Sealed Case, 310 F.3d at 736. The court gave two examples of what it considered to be "non-foreign intelligence information": information about "ordinary crimes" and "scandals." Because the court considered evidence of "ordinary crime" not to be "foreign intelligence information," the court interpreted the FISA to bar the government from using FISA surveillance to obtain evidence of "ordinary crime"—such as bank robbery—unless it was "inextricably intertwined with foreign intelligence crimes." *Id.* at 736. The court was wrong to construe the term "foreign intelligence information" categorically to exclude evidence of "ordinary crime." As discussed above, evidence of ordinary crime can be foreign intelligence information because its use for prosecutorial purposes can serve the protective foreign intelligence purposes identified in the definition of "foreign intelligence information." In concluding otherwise, the court had to create a distinction that the FISA does not recognize and that, indeed, conflicts with the FISA. The court tried to distinguish "foreign intelligence crimes" from "non-foreign intelligence crimes," with the latter excluding "ordinary crimes" that are "inextricably intertwined with foreign intelligence crimes." The FISA does not use any of those terms. More fundamentally, the use of those terms conflicts with Congress's decision in the FISA to authorize the government to obtain "foreign intelligence information" and to define that term to include both criminal and non-criminal conduct. *See infra* note 575–76 and accompanying text.

purpose test. Indeed, it supports the test to the extent of establishing that at least some purposes are improper.

Furthermore, the legislative history contains some statements that seemingly support the judicial primary purpose test even more directly. The FISA Court of Review quoted one such statement. The House report stated that surveillance authorized by the bill that became the FISA "are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information."[538] Other legislative history contains statements similarly indicating that the primary purpose of the surveillance that would be authorized by the FISA was not to get evidence of crime but instead to obtain foreign intelligence information.[539] To similar effect are statements that prosecutions arising from FISA surveillance would be rare.[540] Read in isolation, such statements support the primary purpose test. Understood in context, however, they provide only scant support. As the FISA Court of Review said, these statements reflect "an observation, not a proscription."[541]

Understood in context, such statements reflect congressional awareness that most surveillance for foreign intelligence at the time of FISA's enactment did not produce evidence of crime and was not meant to.[542] Congress heard evidence that most surveillance for

---

[538] *In re* Sealed Case, 310 F.3d at 725 (quoting H.R. REP. NO. 95-1283, at 36 (1978)).

[539] *See, e.g.*, S. REP. NO. 95-604, at 55 (1978) ("Although the primary purpose of electronic surveillance conducted pursuant to this chapter will not be the gathering of criminal evidence, it is contemplated that such evidence will be acquired and [provisions codified in 50 U.S.C. § 1806(b)–(g)] establish the procedural mechanisms by which such information may be used in formal proceedings."); H.R. REP. NO. 95-1283, Pt. 1, at 89 (1978) (same).

[540] *See, e.g.*, 124 CONG. REC. 10897 (1978) (statement of Sen. Wallop) (distinguishing Title III surveillance orders from FISA surveillance orders on the ground that, in the latter context, "We are not trying to catch criminals but to gather information to protect the national interest of the country."); S. REP. NO. 95-604, at 24 n.20 (1978) (stating that bill did not provide for notification of targets of surveillance and commenting, "Such notice is particularly inappropriate in the area of foreign intelligence surveillances, where prosecution is rarely the objective or result."); *id.* at 39 ("Although there may be cases in which information acquired from a foreign intelligence surveillance will be used as evidence of a crime, these cases are expected to be relatively few in number."); S.REP. NO. 95-701, at 41 (1978) (same); H.R. REP. NO. 95-1283, Pt. 1, at 60 (same); *see also* S. REP. NO. 95-701, at 67 (1978) ("It is not contemplated that most electronic surveillance conducted pursuant to this chapter will result in criminal prosecution."); *id.* at 94 (additional views of Sen. Malcolm Wallop) ("Only incidentally some [orders approving electronic surveillance] would result in real trials.").

[541] *In re* Sealed Case, 310 F.3d at 725.

[542] *See, e.g., Church Committee Hearing on the FBI*, *supra* note 64, at 286 (testimony of FBI Director Clarence Kelley) ("[I]ntelligence work involves the gathering of information, not necessarily evidence. The purpose may well be not to prosecute, but to thwart crime or to insure that the Government has enough information to meet any future crisis or emergency."); Lacovara, *supra* note 535, at 124 ("All students of foreign intelligence

foreign intelligence was targeted at foreign powers and official agents of foreign powers, rather than at U.S. persons.[543] Those targets, unlike U.S. persons, were not feasible targets for prosecution. For example, they would have at least colorable claims of sovereign or diplomatic immunity.[544] Furthermore, evidence before Congress also indicated that most intelligence gathering involved plain intelligence rather than counterintelligence ("protective" intelligence).[545] Unlike counterintelligence, which concerns specific foreign threats, plain intelligence usually concerns information that is useful in a more generalized way to the United States' conduct of foreign affairs.[546] Thus, the FISA defined plain intelligence in terms of its relationship to "(A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States"[547] rather

---

agree that much critical information has nothing whatsoever to do with actual or potential crime."); *see also* Zweibon v. Mitchell, 516 F.2d 594, 646 (D.C. Cir. 1975) (stating that national security surveillance "often would not be used for prosecutorial purposes"); *id.* at 648 ("Foreign security wiretaps, even more than domestic security wiretaps, are likely to be aimed at collecting and maintaining 'strategic' intelligence information on a continuing basis rather than at obtaining evidence for use in criminal prosecutions.").

[543] *See, e.g.*, 124 CONG. REC. 28133 (1978) (statement of Rep. Kastenmeier) (stating that "the principal targets" of FISA surveillance were likely to be "not U.S. citizens, but . . . foreign powers, agencies of foreign powers, and others who are not so protected"); S. REP. NO. 95-701, at 9 (1978) ("The primary targets for electronic surveillance to collect foreign intelligence are 'official' foreign powers: (1) foreign governments or their components; (2) factions of foreign nations . . . ; [and] (3) entities which are openly acknowledged by foreign governments to be under their direction and control."); *see also* Lacovara, *supra* note 535, at 122 ("In an intelligence operation . . . information is sought for reasons of state ordinarily unrelated to any criminal investigation.").

[544] *See Senate Judiciary Hearing on FISA*, *supra* note 70, at 31 (testimony of James Adams, Assistant Director, FBI) (stating that most foreign intelligence agencies "have diplomatic status which prevents any prosecution action whatsoever"); *House Intelligence Hearing on FISA*, *supra* note 70, at 29 (reproducing Letter from Justice Department to Chairman of Committee) ("In most cases the target of the proposed surveillance may not be subject to prosecution in the United States, and so the [FISA] proceeding could not in these instances be justified as in aid of the court's jurisdiction over a forthcoming criminal case."); *House Intelligence Hearing on FISA*, *supra* note 70, at 55 (prepared statement of Daniel Murphy, Deputy Under Secretary of Defense for Policy) ("Nearly all, if not all of this information [sought in electronic surveillance conducted or initiated by Department of Defense] would have nothing to do with Americans. It would be sought from electronic surveillance of foreign powers and foreigners who are agents of foreign powers and it would not contain any information concerning Americans.").

[545] *See, e.g.*, *Senate Judiciary Hearing on FISA*, *supra* note 70, at 63 (testimony of Adm. Stansfield Turner, Director of CIA) (stating as a "guess" that electronic surveillance by CIA "is predominantly for the purposes of collecting foreign intelligence, collecting information that will assist us in establishing our political, our military, and our economic policies and assist us in understanding the activities of foreign powers in all three of those fields").

[546] *See* S. REP. NO. 95-604, at 33 (1978) (observing that the portions of definition of "foreign intelligence information" that encompassed positive intelligence bring into the definition "a broader range of material").

[547] 50 U.S.C. § 1801(e)(2) (2003).

than its relationship to specific foreign threats.[548] Because of the more generalized nature of plain intelligence, surveillance for plain intelligence, as distinguished from surveillance for counterintelligence, seldom produced evidence of crime.[549] Finally, evidence before Congress showed that even relatively few surveillances for counterintelligence led to prosecutions.[550] Targets involved in crime often escaped prosecution because the United States decided that prosecution would threaten national security interests, such as by risking the disclosure of U.S. intelligence sources or methods, or that some other approach—such as continued monitoring of the target or an attempt to turn the target into a double agent—would be more productive than prosecution.[551] For this reason, intelligence officials testifying before Congress emphasized that the decision to prosecute targets of counterintelligence should be made by the Attorney General, rather than subordinate prosecutors, after weighing the benefits of prosecution against its possible risks to national security.[552] In short, statements in the legislative history to

---

[548] *Id.* § 1801(e)(1).

[549] *See, e.g.*, *Senate Judiciary Hearing on FISA*, *supra* note 70, at 62 (testimony of Harold Brown, Secretary of Defense) (stating that the issue of "requiring a noncriminal standard for electronic surveillance" is "primarily a counterintelligence problem"); *see also* Hill, *Joint Inquiry Staff Statement*, *supra* note 3, at 23 ("As the 1980s began, the law enforcement and intelligence communities worked together most often in the context of counterintelligence investigations and counternarcotics programs.").

[550] *See, e.g.*, *Senate Judiciary Hearing on FISA*, *supra* note 70, at 31 (testimony of James Adams, Assistant Director, FBI) ("The primary purpose of counterintelligence work is to neutralize the activities of these groups [of alien intelligence agents] to prevent their intelligence-gathering activities, and hardly any of them wind up in prosecutive action."); *id.* at 92–93 (reproducing article by Morton Halperin) (describing two types of electronic surveillance: in surveillance "to gather information about the activities of foreign governments," "[t]here is no suggestion that illegal activity is underway"; in surveillance that tracks an alien foreign agent to an American suspected of being a foreign agent, as well, "arrest and conviction are not usually the objectives").

[551] *See* H.R. REP. NO. 95-1283, Pt. 1, at 36–37 (1978) ("Combating the espionage and covert actions of other nations in this country is an extremely important national concern. Prosecution is one way, but only one way and not always the best way, to combat such activities. 'Doubling' an agent or feeding him false or useless information are other ways. Monitoring him to discover other spies, their tradecraft and equipment can be vitally useful. Prosecution, while disabling one known agent, may only mean that the foreign power replaces him with one whom it may take years to find or who may never be found."); *Senate Judiciary Hearing on FISA*, *supra* note 70, at 32 (testimony of James Adams, Assistant Director, FBI) (explaining his agreement with Sen. Hatch that it is not "always propitious to bust a spy" because, for example, of concerns about disclosure of intelligence sources, methods, and information); *House Intelligence Hearing on FISA*, *supra* note 70, at 119 (statement of Rep. Mazzoli) ("[T]he Department of Defense and the Justice Department have said they are really not trying to nail these people [i.e., the targets of electronic surveillance for foreign intelligence] with a criminal charge anyway. They could care less about scienter. What they are really trying to do is to end the threat or to eliminate these people as foreign agents.").

[552] *See supra* notes 167–69 and accompanying text (discussing requirement for Attorney

the effect that foreign intelligence surveillance was not "primarily" for law enforcement purposes and would only rarely result in prosecution merely reflect the evidence before Congress on existing intelligence practices. The statements do not reflect Congress's intention to impose the judicial primary purpose test.[553]

iii. Legislative History on the "Noncriminal" Standard for FISA Surveillance

Much of the legislative history explained why the bill that became the FISA adopted a so-called "noncriminal standard" to define U.S. persons who were subject to surveillance as "agents of a foreign power." For example, the House report explained the definition of "agent of a foreign power," as applied to U.S. persons, in the passage below. Though lengthy, it provides context for understanding statements about the "primary" purpose of foreign intelligence surveillance:

> Under H.R. 7308 [the House version of the bill signed into law as the FISA], as introduced, there were four categories under the definition of "agent of a foreign power" which could apply to any person, e.g., a United States citizen. One of these categories did not require any showing of possible criminal activity. Another category was a conspiracy provision which, because it referred to the non-criminal standard, could have authorized surveillance of one "conspiring" with someone not engaged in criminal activity. While the witnesses before the [subcommittee that held hearings on the bill] acknowledged that the activity described in the non-criminal standard was "tantamount to a crime," there was apprehension by some that the bill was authorizing electronic surveillance of United States citizens without any explicit showing of criminal activity.
>
> New language was, therefore, developed by the Administration and congressional leaders, with the participation of interested outside parties, including the ACLU.
>
> . . .

General approval).

[553] Apparently reflecting Congress's expectation that FISA surveillance would focus on gathering foreign intelligence information for uses other than prosecution, Congress ultimately provided that the bill that became the FISA would be codified in Title 50 of the U.S. Code, which concerns War and National Defense, instead of Title 18 (relating to Crimes and Criminal Procedure). *See* H.R. REP. NO. 95-1283, Pt. 1, at 28 (1978); *see also* H.R. CONF. REP. 95-1720, at 19 (1978) (stating that the conference rejected the Senate's proposal to put the bill in Title 18 and accepted the House's "uncodified title" so that the bill's provisions would be codified in the part of Title 50 "which most directly relates to its subject matter").

> As a matter of principle, this Committee agrees that no United States Citizen in the United States should be targeted for electronic surveillance by his government absent some showing that he at least may violate the laws of our society. A citizen in the United States should be able to know that his government cannot invade his privacy with the most intrusive techniques if he conducts himself lawfully.
>
> On the other hand, this committee recognizes full well that the surveillance[s] under this bill are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information, which when it concerns United States persons must be necessary to important national concerns. Combating the espionage and covert actions of other nations in this country is an extremely important national concern. Prosecution is one way, but only one way and not always the best way, to combat such activities.[554]

This passage reflects the dilemma that consumed most of the debate on the bills in the 95th Congress that led to FISA.[555] On the one hand, many in Congress believed that U.S. persons should not be subjected to the intrusiveness of electronic surveillance unless they were likely to be involved in criminal conduct.[556] On the other hand,

---

[554] H.R. REP. NO. 95-1283, pt. 1, at 36–37 (1978).

[555] *See, e.g.*, 124 CONG. REC. 10887–88 (1978) (statement of Sen. Kennedy) (stating that "a major stumbling block" to enactment of legislation in 94th Congress was its inclusion of a non-criminal standard, and that "the major breakthrough" of S. 1566, 95th Cong. (1977) was its resolution of "the issue of the so-called noncriminal standard"); *id.* at 10890 (statement of Sen. Bayh) (stating that the criminal standard was "probably the most controversial, the most sensitive, and yet probably the most important aspect of this legislation"); *id.* at 28142 (statement of Rep. Drinan) ("H.R. 7308 does not uniformly require a criminal standard. That is its major deficiency . . . "); S. REP. NO. 95-604, at 17 (1978) ("A difficult issue posed during committee deliberations was whether foreign intelligence electronic surveillance should be limited to situations involving the commission of a crime."); *id.* at 83 (minority views of Sen. James Abourezk) (stating that "noncriminal standard" for identifying permissible U.S. person-targets of FISA surveillance makes bill "fatally defective"). Indeed, legislation similar to the FISA died in the 94th Congress largely because it prescribed a "noncriminal" standard for surveillance. Legislation in the 94th Congress defined an "agent of a foreign power," the term that identifies a proper target of surveillance, to include a U.S. person who, under certain circumstances, covertly gives information to foreign intelligence officials. S. 3197, 94th Cong. (1977). Opponents of that provision criticized it as allowing a "noncriminal" standard for surveillance that raised Fourth Amendment concerns. *See, e.g., Senate Intelligence Hearing on FISA*, *supra* note 70, at 5 (statement of Sen. Morgan) (saying that he had voted against S. 3197, 94th Cong. (1977) partly because he was "disturbed about the lack of criminal standards" for surveillance); *id.* at 14 (prepared statement of Attorney General Griffin Bell) ("In response to last year's bill, a concern was expressed involving the so-called non-criminal standard for the definition of an agent of a foreign power."); *Senate Judiciary Hearing on FISA*, *supra* note 70, at 80 ("The absence of a crime standard was one of the principal issues on which S. 3197 foundered.").

[556] *Senate Intelligence Hearing on FISA*, *supra* note 70, at 8 (reproducing Additional Views of Sen. Biden on S. 3197, 94th Cong. (1977)) ("The scheme the founding fathers

a pure criminal standard for targeting U.S. persons ignored that evidence of criminal conduct does not identify every U.S. person who, from a foreign intelligence perspective, should be targeted for surveillance; U.S. persons could warrant surveillance for conduct that was totally innocent or, at least, not a crime.[557]

This and similar passages show that Congress and groups interested in the legislation understood that some foreign intelligence surveillance would reveal evidence of crime that would be used for prosecution.[558] Prosecution became all the more likely as Congress

---

developed, in the Fourth Amendment, to police invasions of privacy has two basic parts. First, an American's privacy cannot be invaded unless a judicial officer issues a warrant authorizing the search, and second, the judge must have probable cause to believe that the search will seize particular evidence of specific criminal activity."); *id.* at 14 (prepared statement of Attorney General Griffin Bell) (stating his belief that objections to narrowly drawn noncriminal standard were based on view that "as a matter of principle a United States person should not be made a target of an electronic surveillance unless there is probable cause to believe he has violated the law."); *id.* at 55 (statement of Sen. Morgan) (stating as a general matter, "I am inclined to believe . . . that there ought to be a criminal standard, . . . either the person is committing a crime or is about to commit a crime.").

[557] For example, when FISA was enacted it was not a crime for someone in this country to plan a terrorist attack overseas, yet the government wanted to be able to conduct surveillance of such a person, partly to fulfill international obligations. *See* H.R. REP. NO. 95-1283, Pt. 1, at 43 (1978) (citing the terrorist "Carlos" as an example of someone who "may not have violated U.S. law, even though they may have murdered hundreds of persons abroad."); *id.* at 45 ("The committee intends that terrorists and saboteurs acting for foreign powers should be subject to surveillance under this bill when they are in the United States, even if the target of their violent acts has been within a foreign country and therefore outside actual Federal or State jurisdiction. This departure from a strict criminal standard is justified by the international responsibility of governments to prevent their territory from being used as a base for launching terrorist attacks against other countries as well as to aid in the apprehension of those who commit such crimes of violence.").

[558] *See, e.g.*, 124 CONG. REC. 10887 (1978) (statement of Sen. Kennedy) (stating that bill "mandates that before any information obtained can be used at a subsequent criminal trial, the trial court must . . . find that all statutory wiretap procedures have been met."); S. REP. NO. 95-701, at 10–11 (1978) ("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 . . . . Intelligence and criminal law enforcement tend to merge in this area.") (footnote omitted); *id.* at 14 ("Foreign counterintelligence surveillance may target U.S. persons and may involve detection of crimes, even though criminal prosecution may not result."); H.R. REP. NO. 95-1283, Pt. 1, at 49 (1978) (observing that information "about a spy's espionage activities" falls within the definition of "foreign intelligence information" "and it is most likely at the same time evidence of criminal activities"); *Senate Intelligence Hearing on FISA*, *supra* note 70, at 42 (statement of Sen. Garn) (observing that *ex parte* nature of proceeding for judicial authorization of electronic surveillance under FISA was justified by need to avoid disclosure that would "make prosecution impossible"); *id.* at 128 (testimony of Morton Halperin, Center for National Security Studies) (stating that bill violates the principle that "if a criminal defendant would be entitled to information which the Government declines to release on national security grounds, the Government faces the choice of making the information available or dropping the prosecution" because the bill "suggests that even if the Government intends to use the fruits of a national security electronic surveillance in a criminal case, it need not turn over the [judicial] authorization to the defendant unless the court finds that that is necessary"); *id.* at 133 (prepared statement of Steven Rosenfeld, Comm. on Fed. Legislation, Ass'n of Bar of NYC) (citing among the Committee's "major

refined the definition of "agent of a foreign power" so that it mostly applied to U.S. persons only if they were involved in crime. Indeed, the legislative history shows Congress approved prosecution as one way "to combat" the "espionage and other covert actions of other nations in this country."[559] To Congress, it was "[o]bvious[]" that "use of 'foreign intelligence information' as evidence in a criminal trial is one way the Government can lawfully protect against clandestine intelligence activities, sabotage, and international terrorism."[560] Accordingly, Congress clearly would have approved of FISA surveillance conducted for the "primary purpose" of getting evidence of crime if the government reasonably believed that prosecution was the best way to combat the foreign threat that the government wanted to surveil. As discussed above, it does not matter that, at the time of the original FISA's enactment, the government rarely determined that prosecution was the best way to achieve foreign intelligence purposes.[561]

Indeed, opponents of a non-criminal standard for FISA surveillance of U.S. persons did not use the prospect of criminal prosecution as an argument for imposing the judicial primary purpose test. They used the prospect of prosecution as an argument for adopting a criminal standard for U.S. persons and putting other restrictions on such surveillance.[562] Furthermore, they did not cite the risk of prosecution

---

concerns" "[t]he possibility that the bill may be read to sanction the use of evidence obtained by foreign intelligence surveillance in criminal and other proceedings based only upon *ex parte* determinations"); *id.* at 234–36 (appendix to letter from Attorney General Griffin Bell prescribing guidelines for dissemination of evidence of crime collected during intelligence and counterintelligence investigations); *Senate Judiciary Hearing on FISA*, *supra* note 70, at 65 (statement of Sen. Abourezk) ("The evidence gathered under the noncriminal standard of this proposed legislation can be used for prosecution in criminal cases.").

[559] H.R. REP. NO. 95-1283, pt. 1, at 36 (1978).

[560] *Id.* at 49.

[561] *See supra* notes 550–51 and accompanying text.

[562] *See, e.g.*, *Senate Judiciary Hearing on FISA*, *supra* note 70, at 34–35 (statement of Sen. Abourezk) (arguing that it violated Fourth Amendment to use in a criminal proceeding information obtained through surveillance authorized under a noncriminal standard); *House Intelligence Hearing on FISA*, *supra* note 70, at 130 (prepared statement of Robert Sheehan, Comm. on Federal Legislation, Ass'n of Bar of NYC) (citing among the Committee's "major concerns" "[t]he possibility that the bill may be read to sanction the use of evidence obtained by foreign intelligence surveillance in criminal and other proceedings based only upon *ex parte* determinations, without any adversary hearing of any kind"); *id.* at 145 (testimony of Morton Halperin, Project on National Security) (arguing that because foreign intelligence surveillance could lead to evidence of crime to be used in criminal prosecutions, the Constitution required disclosure to the defendant of the warrant and fruits of the search); *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings on S. 3197 before the Subcomm. on Intelligence and the Rights of Americans of Senate Select Comm. on Intelligence*, 94th Cong., 2d Sess. 95 (1976) (statement of Sen. Bayh) (expressing concern that, under predecessor bill "we

as their main argument for a criminal standard. Their main argument for the criminal standard was that electronic surveillance itself was burdensome quite apart from the danger of prosecution i.e., it is or can be hurtful, intrusive, and fraught with dangers such as revelation of embarrassing personal information or the threat of such revelation as a means of harassment.[563] The intrusiveness of electronic surveillance was often cited by supporters of a criminal standard to distinguish electronic surveillance from cases in which the Supreme Court had upheld against Fourth Amendment attack administrative inspections and other searches conducted under noncriminal standards.[564] Supporters of a criminal standard for electronic surveillance thus argued that a citizen should be subject to the

---

are establishing a standard . . . which not only permits surveillance be logged for the collection of information which may be necessary for the protection of this country, but also . . . to be used subsequently for criminal prosecution without the probable cause standard which is now required.").

[563] *See, e.g.*, S. REP. NO. 95-604, at 84 (1978) (minority views of Sen. James Abourezk) (referring to "the pervasive type of search which electronic surveillance entails" to explain his view that a U.S. person should not be targeted for such surveillance without probable cause to believe he or she was committing a crime); *Senate Intelligence Hearing on FISA*, *supra* note 70, at 92 (prepared statement of Prof. Christopher Pyle) (arguing that same Fourth Amendment requirements should apply to surveillance for law enforcement purposes and surveillance for foreign intelligence purposes because "[b]oth are equally intrusive"); *id.* at 112 (prepared statement of John Shattuck and Jerry Berman, ACLU) ("Why is it so important to limit the wiretapping authorized by H.R. 7308 to a 'criminal standard'? A wiretap is probably the most intrusive and inherently unreasonable form of search and seizure. Even when a tap is placed on a person suspected of engaging in criminal activity, it offends the Fourth Amendment because it necessarily results in a 'general search'"); *id.* at 78 (prepared statement of John Shattuck, ACLU) ("Since electronic surveillance is inherently so intrusive, the ACLU has long maintained that it cannot be conducted at all without violating the Fourth Amendment. If this violation is to be minimized, at the very least no surveillance should be authorized unless there is probable cause to believe that the person to be tapped is engaged in crime."); *House Intelligence Hearing on FISA*, *supra* note 70, at 81 (prepared statement of John Shattuck and Jerry Berman, ACLU) (substantially identical to prepared statement, quoted *supra* this note, submitted at Senate hearings); *id.* at 233 (testimony of Ambassador Laurence Silberman) (argument for criminal standard "is based on the notion that surveillance is a punishment, and therefore it should only apply to people who commit crimes"); *see also* Cinquegrana, *supra* note 58, 137 U. PA. L. REV. at 809–10 (stating that proponents of criminal standard "argued that electronic surveillance should be limited to cases involving violations of criminal law since it is generally intrusive and inherently results in the acquisition of many irrelevant communications") (footnote omitted).

[564] *See, e.g.*, *Senate Judiciary Hearing on FISA*, *supra* note 70, at 79 (prepared statement of John Shattuck, ACLU) (distinguishing administrative searches from electronic surveillance for foreign intelligence information on the ground that the latter involve "a deliberate search for information *unrelated* to criminal activity" (emphasis added), and that cases on administrative searches "deal with a much less intrusive invasion of privacy"); *House Intelligence Hearing on FISA*, *supra* note 70, at 108 (testimony of John Shattuck, ACLU) ("The distinction between the OSHA case [involving administrative searches] and the wiretaps before us in this bill is that the degree of intrusion is far less serious and the Supreme Court has generally upheld administrative searches, sometimes with a warrant, but always pegged on the degree of intrusion.").

extraordinary intrusion of electronic surveillance only if their conduct created probable cause of crime.[565] By the same token, "A citizen . . . should be able to know that his government cannot invade his privacy with the most intrusive techniques if he conducts himself lawfully."[566]

True, some opponents of the FISA worried that prosecutors would use it to avoid the traditional requirements for warrants to obtain evidence of crime.[567] They expressed this worry, however, to explain why Congress should impose stringent requirements for the government to get judicial authorization for surveillance under the FISA.[568] The idea was that the government would not use FISA to avoid the traditional requirements for law-enforcement surveillance if FISA's requirements for foreign intelligence surveillance were

---

[565] *See, e.g.*, S. REP. NO. 95-604, at 84 (1978) (minority views of Sen. James Abourezk) ("I believe, as the Church committee found, that 'as a matter of principle . . . an American ought not to be targeted for surveillance unless there is probable cause to believe that he may violate the law.'") (quoting *Church Committee Final Report*, *supra* note 62, at 325).

[566] H.R. REP. 95-1283, Pt. 1, at 36 (1978).

[567] *Senate Intelligence Hearing on FISA*, *supra* note 70, at 139 (prepared statement of Steven Rosenfeld, Comm. on Fed. Legislation, Ass'n of Bar of NYC) ("We are concerned that [the provision in the bill] which provides that minimization procedures shall not be deemed to preclude retention and disclosure of information incidentally acquired which is evidence of a crime might permit law enforcement agencies to conduct illegal domestic surveillance under the guise of foreign intelligence surveillance, where they cannot meet a 'probable cause' standard to obtain warrants for surveillance."); *Senate Judiciary Hearing on FISA*, *supra* note 70, at 34–35 (statement of Sen. Abourezk) (distinguishing surveillance under Title III from surveillance under proposed legislation on the ground that Title III imposes a criminal standard); *House Intelligence Hearing on FISA*, *supra* note 70, at 147 (testimony of Robert Sheehan, Comm. on Fed. Legislation, Ass'n of Bar of NYC) (expressing Committee's "fear that in the future a law enforcement purpose might be attempted to be served in a case where there is no probable cause showing of criminal activity under the normal standards for obtaining a warrant").

[568] *Senate Intelligence Hearing on FISA*, *supra* note 42, (prepared statement of Steven Rosenfeld, Comm. on Fed. Legislation, Ass'n of Bar of NYC) (stating that, to prevent use of FISA for law enforcement purposes when traditional probable cause standard cannot be met:

> [T]he bill should contain an additional proviso that information or evidence incidentally obtained in the course of foreign intelligence surveillance, while it may be disclosed to the appropriate domestic law enforcement agencies, would remain subject to all of the established statutory and Fourth and Fifth Amendment protections and restrictions upon admission into evidence or other use in the criminal law enforcement process.)

Senate Judiciary Hearing on FISA, *supra* note 70, at 34–35 (statement of Sen. Abourezk) (expressing concern about the noncriminal standard for electronic surveillance under proposed legislation, and distinguishing it from Title III's criminal standard for surveillance, in discussing what standard and safeguards Congress should ultimately prescribe for surveillance under the proposed legislation); *House Intelligence Hearing on FISA*, *supra* note 70, at 147 (testimony of Robert Shaheen, Comm. on Fed. Legislation, Ass'n of Bar of NYC) (arguing that the requirement for judicial approval under proposed legislation should be made stricter, based on the committee's fear that government might use surveillance authority under proposed legislation for "a law enforcement purpose").

comparably stringent. Concern about circumvention of the traditional requirements for law-enforcement surveillance was generally not used to argue that Congress should bar the government from using FISA surveillance for law enforcement purposes.[569] Maybe this is because the Church Committee did not reveal, among the significant abuses of the past, the use of "national security" surveillance as a pretext for surveillance, the "primary purpose" of which was really to get evidence of crime.[570]

By the same token, people appearing before the 95th Congress who favored a noncriminal standard for FISA surveillance did not claim that the government would never conduct FISA surveillance for the primary purpose of getting evidence of crime. Instead, they argued that tying FISA surveillance to a criminal standard was too restrictive to accommodate legitimate government intelligence interests.[571]

---

[569] For the only exception to the statement in the text that this author discovered, see 124 CONG. REC. 28142 (1978) (statement of Rep. Drinan):

> When Government agents obtain incriminating evidence through electronic surveillance not intended for that purpose and which may be totally unrelated to the alleged criminal activity, they should not be allowed to use it for prosecutorial purposes. Such 'fruit of the forbidden tree' should not be available to prosecute the party for conduct which may not be even remotely connected to the object of the surveillance. This is especially true when it is considered that the criminal standard, where it does appear in these bills, is not uniformly required for obtaining a surveillance warrant in the first instance.

House Intelligence Hearing on FISA, *supra* note 70, at 196 (prepared statement of Rep. Drinan) (essentially identical to statement on floor of Congress). Two features of this statement deserve attention. First, it objects to the use of information to prosecute only crimes that are "totally unrelated" to the object of the surveillance. Second, it bases this objection in part on the absence of a uniform "criminal" standard for surveillance, an objection that Congress considered and rejected. 50 U.S.C. § 1801(h)(3). In addition to Representative Drinan's statement, some case law involving pre-FISA surveillance expressed concern that the government would invoke "national security" to avoid the traditional probable cause requirement for electronic surveillance. *See, e.g.*, Zweibon v. Mitchell, 516 F.2d 594, 609 n.23 (D.C. Cir. 1975) (noting "the potential for abuse of [warrantless electronic surveillance conducted in the name of national security] as a means for circumventing the warrant requirement in normal criminal investigations").

[570] *See generally Senate Intelligence Hearing on FISA*, *supra* note 42, at 261–87 and 288–315 (reproducing portions of Church Committee report addressing "excessive use of intrusive techniques" and "political abuse of intelligence information"); *see also Zweibon*, 516 F.2d at 612 n.39 (noting that wiretap authorizations in that case "ordered that evidence derived therefrom not be used for prosecutorial purposes"); *cf. Church Committee Final Report*, *supra* note 64, book II, at 161–62, 189–90 & n.30 (reporting instance in which a federal law enforcement agency, the Bureau of Narcotics and Dangerous Drugs, asked the National Security Administration to monitor telephone calls between New York City and a city in South America because of the Bureau's doubt that it could itself legally tap the telephones).

[571] *See* 124 CONG. REC. 10889 (1978) (statement of Sen. Garn) (stating that he supported a noncriminal standard because, among other reasons, "the desire to use surveillance-obtained information to uncover a wider network of foreign agents often prevents prosecution; and . . . the Government may not desire prosecution since to do so would require them to reveal even more sensitive information in a court proceeding"); *id.*

There were circumstances when surveillance was justified—of an "innocent dupe," for example—even though the target was not involved in crime.[572] Supporters of the noncriminal standard for

---

at 28166 (statement of Rep. McClory) (arguing that criminal standard was too narrow because it ignored that "most intelligence relates not to criminal activities, but solely to the subject of gathering information which may be useful to our Nation"); S. REP. NO. 95-604, at 25 (1978) ("Although the [Carter] Administration is committed to using the criminal standard [for electronic surveillance] wherever possible, there are several situations" where that is not possible); *id.* ("Because of this range of cases, which may or may not fall within the ambit of the espionage laws, but do involve Americans working for a foreign intelligence service under circumstances dangerous to national security, the Committee has chosen to include this limited noncriminal standard for Americans."); *Senate Intelligence Hearing on FISA*, *supra* note 70, at 15 (statement of Attorney General Griffin Bell) (discussing situations in which foreign intelligence surveillance of Americans' activity was justified "whether or not that activity is today a violation of our criminal statutes"); *Senate Judiciary Hearing on FISA*, *supra* note 70, at 11 (statement of Sen. Thurmond) (stating: "There is no requirement in this bill . . . that the target of the surveillance be actually engaged in the commission of a crime. Nor should there be such a requirement."; and giving example of when surveillance was justified of activity that "is generally not illegal"); *id.* at 37 (statement of Sen. Hatch) (identifying "certain acts that do not rise to the nature of a crime under our present criminal laws but necessarily become essential to our security interests"); *House Intelligence Hearing on FISA*, *supra* note 70, at 3 (prepared statement of Rep. McClory) (advocating legislation that would not require prior judicial approval for foreign intelligence surveillance because of "the differences in the circumstances which necessitate 'searches and seizures' for law enforcement and those necessary for foreign intelligence gathering"); *id.* at 208 (prepared statement of Philip Lacovara) (stating that requiring a pure criminal standard for surveillance would cause "much of the rationale" for the proposed legislation to "evaporate"; and explaining that "[t]he whole point" of the proposed legislation is gathering foreign intelligence and is premised on the principle that "the government has a legitimate need for information relating to our foreign relations and national defense even though the sources of that information may not be personally involved in criminal conduct").

[572] *See* S. REP. NO. 95-701, at 95–96 (1978) (additional views of Sen. Malcolm Wallop):

> In cases where the defense of foreign relations of the United States are concerned, the subject's [i.e., surveillance target's] culpability or responsibility is arguably beside the point. The information gained by surveilling him may not relate to him at all, but may save countless lives . . . . Consider . . . the case of a thoroughly innocent American who may have knowledge which, unbeknownst to him, would shed light on foreign military or intelligence plans, and who would be placed in danger if contacted [directly by government officials]. Under this bill this American could not be surveilled.

Id.; *House Intelligence Hearing on FISA*, *supra* note 70, at 213 (testimony of Philip Lacovara) ("I think there may be a number of situations in which American citizens, perhaps acting in good faith, or at least acting short of the criminal culpability line, may be the permissible subjects of intelligence gathering by the Government."); *id.* at 233 (testimony of Ambassador Laurence Silberman) ("[T]here are certain hypotheticals . . . where perfectly innocent people may have to be surveilled, and where I think it is justifiable."); *see also Senate Judiciary Hearing on FISA*, *supra* note 70, at 8–10 (reproducing appendix to letter from Attorney General Griffin Bell to Sen. Abourezk describing six hypothetical situations in which electronic surveillance for foreign intelligence was warranted even though target of surveillance may not be involved in criminal conduct); *cf.* S. REP. NO. 95-604, Pt. 2, at 1–4 (1978) (appendix to the minority views of Sen. James Abourezk) (discussing hypothetical situations submitted by the Department of Justice to Congress to demonstrate need for "noncriminal" standard for electronic surveillance for foreign intelligence); *Senate Intelligence Hearing on FISA*, *supra* note 70, at 93–97 (prepared statement of Prof. Christopher Pyle) (same); *id.* at 119–21 (prepared statement of John Shattuck and Jerry Berman, ACLU) (same).

surveillance believed that national security interests sometimes justified surveillance of even innocent U.S. persons.[573] At the same time, they emphasized that the noncriminal standard proposed in the bills that became the FISA were very narrow. In almost all cases a U.S. person could be targeted for FISA surveillance only for violating the law.[574] Congress ultimately sided with national security interests to the extent that it defined "agent of a foreign power," as applied to U.S. persons, by reference to some noncriminal conduct.[575] Congress also, however, acknowledged civil liberty concerns by making the definition come as close as possible to requiring a finding of criminal conduct without sacrificing national security.[576]

---

[573] H.R. REP. NO. 95-1283, Pt. 1, at 118 (dissenting views on H.R. 7308) (1978):

When the Government seeks evidence to support a prosecution, it may be reasonable to require that the probable cause standard apply to the issue of criminality itself. Where, however, the object of the government is to gather intelligence related to national security or defense of the country, the situation is very different.

Whether the activities which the President may wish to scrutinize are illegal or not is not of primary importance, for the government does not seek the information to prosecute. While prosecution may prove to be a viable option, the main thrust of our efforts in this area are to protect against foreign intelligence activities which threaten our security. Prosecution may be, as most often has been the case, inappropriate or harmful to that effort. To impose a criminal standard, therefore, adds a requirement, not mandated by the Constitution, which could in fact inhibit powers reserved to the Executive.

[574] *See, e.g.*, *Senate Intelligence Hearing on FISA*, *supra* note 70, at 17 (prepared statement of Attorney General Griffin Bell) ("Under S. 1566 in almost all cases an American will have to be violating Federal law to be targeted for electronic surveillance."); *Senate Judiciary Hearing on FISA*, *supra* note 70, at 66 (reproducing letter from Justice Department to Sen. Kennedy's staff, stating that "[t]he non-criminal standard is a very narrow exemption").

[575] *See* S. REP. NO. 95-701, at 12–13 (1978):

> The essential point is that, if electronic surveillance is to make an effective contribution to foreign counterintelligence, it must be available for use when necessary for the investigative process. The criminal laws are enacted to establish standards for arrest and conviction; and they supply guidance for investigations conducted to collect evidence for prosecution. Foreign counterintelligence investigations have different objectives. They succeed when the United States can insure that an intelligence network is not obtaining vital information, that a suspected agent's future access to such information is controlled effectively, and that security precautions are strengthened in areas of top priority for the foreign intelligence service. Prosecution is a useful deterrent, but only where the advantages outweigh the sacrifice of other interests. Therefore, procedures appropriate in regular criminal investigations need modification to fit the counterintelligence context.

Id. (defending the noncriminal standard).

[576] Early versions of the bills that became the FISA authorized electronic surveillance of U.S. persons in two situations that were not defined necessarily to involve criminal conduct. One was for a U.S. person who:

> pursuant to the direction of an intelligence service or intelligence network of a foreign power, knowingly collects or transmits information or material to an intelligence service or intelligence network of a foreign power in a manner intended to conceal the nature of such information or material or the fact of such transmission or collection, under circumstances which indicate the transmission

iv. Scarcity of Legislative History Citing Primary Purpose Case Law

The last aspect of the legislative history that is relevant to the validity of the judicial primary purpose test as a gloss on FISA is the legislative history's almost complete failure to mention the primary purpose test then extant in the case law.[577] As discussed above, the primary purpose test began as a judicially conceived Fourth Amendment limit on warrantless electronic surveillance by the government. The leading cases are *Brown* and *Butenko*. Only after FISA's enactment did courts transform this Fourth Amendment test

---

> of such information or material would be harmful to the security of the United States, or that the lack of knowledge by the United States of such collection or transmission would be harmful to the security of the United States.

S. REP. NO. 95-604, at 17 (1978). "This standard was also present in S. 3197, [94th CONG. (1976)] except for the addition of collection to the activities which would justify surveillance." *Id.* The other situation allowed surveillance of a U.S. person who conspired with or aided or abetted someone who engaged in the conduct described in the first situation; or someone who "knowingly engages in clandestine intelligence activities for or on behalf of a foreign power under circumstances which indicate that such activities would be harmful to the security of the United States." S. REP. NO. 95-604, at 17 (1978). The committees refined the definition of "agent of a foreign power," as applied to U.S. persons generally to minimize the situations in which the definition would apply without reference to actual or potential criminal conduct. *See* S. REP. NO. 95-701, at 21–26 (1978) (discussing extent to which criminal conduct would be involved in situations covered by portion of definition of "agent of a foreign power" that dealt with certain clandestine intelligence gathering and other clandestine intelligence activities); H.R. REP. NO. 95-1283, Pt. 1, at 36 (1978) (defining agent of a foreign power through compromise language that "requires that whenever a United States person is to be the target of a surveillance there must be a showing that his activities at least may involve a violation of law"); *id.* at 39 (explaining that the inclusion of conduct that "may involve" a crime in the definition of "agent of a foreign power" reflected committee's judgment "that it is necessary in order to permit the Government to investigate adequately" in certain cases where crime could not be proven); *see also* 124 CONG. REC. 10900 (1978) (statement of Sen. Church) ("In the case of this bill, we have established a criminal standard as in ordinary criminal cases."); *id.* (statement of Sen. Bayh) ("In structuring the criminal standard, we have used words which we feel are as close to the words of art as we can, to give flexibility to those who need to get involved in the use of some of this technology which is now available to protect our country but to nevertheless apply that perhaps a bit broader standard to the criminal test which I think is basic to our system in this country."); *Senate Intelligence Hearing on FISA*, *supra* note 70, at 9 (additional views of Sen. Biden on S. 3197, 94th Cong. (1976)) (observing that in negotiations Attorney General had agreed to changes "so that before authorizing electronic surveillance the judge must be satisfied that the American is engaged in specific acts, with very limited exceptions, criminal acts"); *id.* at 190–92 (statement of Sen. Bayh) (discussing committee amendment that would narrow "noncriminal" standard for identifying U.S. person-agents of foreign powers who could be targeted for surveillance); *House Intelligence Hearing on FISA*, *supra* note 70, at 37–38 (testimony of Attorney General Griffin Bell) (stating that one portion of proposed definition of "agent of a foreign power" was "as near to a criminal standard as anything could be" and that activity covered is "tantamount to a crime"); *House Intelligence Hearing on FISA*, *supra* note 70, at 207 (prepared statement of Philip Lacovara) (expressing the view that the proposed definition of "agent of a foreign power" as applied to U.S. persons is constitutional because it "comes quite close to requiring a showing of criminal involvement").

[577] *See infra* notes 579–81.

into a restriction imposed by the FISA's purpose provision.[578]

Butenko, like *Brown*, is cited in the legislative history of the original FISA. Indeed, the legislative history often cites them together.[579] In only a couple of instances, however, are those citations accompanied by an explicit mention of the primary purpose test. For example, a senate committee report describes *Butenko* as holding that "electronic surveillance conducted without a warrant would be lawful so long as the primary purpose was to obtain foreign intelligence information."[580] The same report, however, found that "[n]either *Brown* nor *Butenko* provide a systematic analysis" of the constitutionality of warrantless electronic surveillance for foreign intelligence.[581] Furthermore, none of the legislative history's references to *Brown* and *Butenko* cite them to suggest that the bills that would become FISA imposed the judicial primary purpose test. The legislative history's failure to do so suggests that Congress did not intend the FISA to impose that test.

Indeed, Congress may well have believed that *Butenko* and *Brown* did not support imposing the judicial primary test on surveillance authorized by the FISA because that test was designed for warrantless surveillance, i.e., surveillance conducted without prior judicial approval.[582] Although the orders approving surveillance under the bills that became the FISA were not called "warrants," that did not reflect a judgment that they were not "warrants" within the meaning of the Fourth Amendment.[583] It reflected, instead, that the drafters of the FISA used Title III as a model, and Title III did not use the term "warrants."[584] Even so, Congress considered FISA surveillance

---

[578] *See supra* notes 171–223 and accompanying text.

[579] S. REP. NO. 95-604, at 14–15 (1978); S. REP. NO. 95-701, at 9 n.3 (1978); H.R. REP. NO. 95-1283, Pt. 1, at 114–15 & n.13 (1978) (dissenting views on H.R. 7308); *cf.* S. REP. NO. 95-604, at 58 (1978) (citing *Butenko* for its discussion of whether information underlying electronic surveillance needs to be disclosed to a defendant against whom the government seeks to use evidence obtained through the surveillance); S. REP. NO. 95-701, at 64 (1978) (same); *Senate Judiciary Hearing on FISA*, *supra* note 70, at 10–11 (statement of Sen. Thurmond).

[580] S. REP. NO. 95-604, at 14–15 (1978).

[581] S. REP. NO. 95-604, at 15 n.26 (1977).

[582] *See supra* notes 171–209 and accompanying text.

[583] *See, e.g.*, S. REP. NO. 95-604, at 5 (1978) ("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."); H.R. REP. NO. 95-1283, Pt. 1, at 27 (1978) (referring to the bill's "warrant requirement").

[584] *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings on S. 3197 Before the Subcomm. on Intelligence and the Rights of Americans of Senate Select Comm. on Intelligence*, 94th CONG., 2d Sess. 77 (1976) (statement of Attorney General Edward Levi) (saying, of predecessor bill, that its standards and

orders tantamount to warrants requiring a criminal standard for issuance,[585] which made surveillance conducted under them quite different from the warrantless surveillance at issue in the case law interpreting the Fourth Amendment to impose the primary purpose test. By the same token, congressional debate on the FISA contains few or no references to surveillance under the FISA as equivalent to warrantless surveillance.[586] Indeed, a big selling point of the FISA was that it required prior judicial approval for electronic surveillance under legislative standards.[587]

2. Provisions on Minimization Procedures

The FISA Trial Court relied on the FISA provisions on

---

procedures, "particularly its provision for prior judicial approval, draw upon the traditional criminal law enforcement search warrant model, the pattern followed in Title III").

[585] *See, e.g.*, 124 CONG. REC. 10887 (1978) (statement of Sen. Kennedy) ("The bill would require that all foreign intelligence electronic surveillance in the United States . . . be subject to a judicial warrant requirement based on probable cause."); *id.* at 10897 (statement of Sen. Abourezk):

> For the first time, warrants will be required in the area of foreign intelligence electronic surveillance . . . . In every instance in which a warrant can be issued against an American citizen . . . the Government must demonstrate . . . that a nexus exists between the activities of the citizen and a violation of the criminal laws.

Id.; *id.* at 28125–26 (1978) (statement of Rep. Murphy) (stating that, with limited exceptions, "[t]he bill would require a prior judicial warrant for all electronic surveillance for foreign intelligence purposes" and that the criminal standard was required to get the warrant); *Senate Intelligence Hearing on FISA*, *supra* note 42, at 111 (prepared statement of John Shattuck and Jerry Berman, ACLU) (stating preference for H.R. 7308, which was the House version of bill that became the FISA, because, unlike a competing bill, H.R. 7308 contained the "requirement that all such wiretaps be conducted pursuant to a judicial warrant" and because of H.R. 7308's "specificity as to the showing the Government must make to obtain a warrant"); *id.* at 132 (prepared statement of Steven Rosenfeld, Comm. on Fed. Legislation, Ass'n of Bar of NYC) ("The judicial warrant procedure established by S. 1566 is certainly a major step in th[e] direction" of legislation "needed to protect individuals . . . from intrusion upon their fundamental rights and liberties."); *Senate Judiciary Hearing on FISA*, *supra* note 70, at 57 (prepared statement of Adm. Stansfield Turner, Director of CIA) ("I accept . . . the warrant requirement that is the central feature of the bill.").

[586] *Cf. Senate Intelligence Hearing on FISA*, *supra* note 42, at 88–89 (prepared statement of Prof. Christopher Pyle) (arguing that because of deviance from traditional probable cause, the bill provided for "pseudo-warrants").

[587] *See, e.g.*, 124 CONG. REC. 10888 (1978) (statement of Sen. Garn) (stating that the bill "for the first time brings all electronic surveillance conducted within the United States under judicial review"); S. REP. NO. 95-604, at 6 (1978) (stating that S. 1566, 95th Cong. (1977), increased protection for U.S. persons compared to S. 3197, 94th Cong. (1976), by authorizing limited judicial review); *id.* at 15 (stating that S. 1566 "would relegate to the past the wire-tapping abuses brought to light during the committee hearings by providing, for the first time, effective substantive and procedural statutory controls over foreign intelligence electronic surveillance."); *Senate Intelligence Hearing on FISA*, *supra* note 42, at 2–3 (statement of Sen. Bayh) (citing S. 1566's provision for "judicial review of the executive certification that surveillance of an American is necessary to obtain foreign intelligence information" as one "significant change[]" from S. 3197).

minimization procedures, rather than on the original FISA's purpose provision, to reject a large portion of the March 2002 information-sharing procedures adopted by the Attorney General.[588] The FISA Court of Review reversed the FISA Trial Court, holding, with little analysis, that the minimization procedures provided "no basis" for the trial court's decision.[589] This subsection offers an analysis that, it is hoped, clarifies why the trial court erred in relying on the minimization procedures.

a. Text of FISA Provisions on Minimization Procedures

The FISA Trial Court rejected the Attorney General's 2002 procedures because, and to the extent that, they were "designed to enhance the acquisition, retention, and dissemination of *evidence for law enforcement purposes, instead* of being consistent with the need of the United States to 'obtain, produce, and disseminate *foreign intelligence information*.'"[590] The court found this design "consistent with the government's interpretation of the recent amendments that FISA may now be 'used *primarily* for a law enforcement purpose.'"[591] For that very reason, in the court's view, the procedures were not "'consistent' with the need to obtain, produce, and disseminate *foreign intelligence information*."[592] The court's own italics show that it forcefully (and forcibly) distinguished (1) procedures designed to facilitate the gathering and processing of criminal evidence from (2) procedures designed to facilitate the gathering and processing of foreign intelligence information. The court rejected the March 2002 procedures to the extent that they served the first function "*instead of*" the second.[593] The FISA Court of Review faulted this reasoning as resting on the same false dichotomy between foreign intelligence and law enforcement as underlay earlier primary purpose case law.[594] But the flaw goes

[588] *See In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 616–25 (Foreign Int. Surv. Ct. 2002); *see also supra* notes 330–40 and accompanying text (discussing FISA Trial Court's opinion).

[589] *In re* Sealed Case, 310 F.3d 717, 731 (Foreign Int. Surv. Ct. Rev. 2002).

[590] *In re All Matters Submitted to Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d at 623 (emphasis in original).

[591] *Id.*

[592] *Id* at 622 (emphasis in original).

[593] *Id.* at 624 (emphasis in original).

[594] *See In re* Sealed Case, 310 F.3d at 721 (stating that FISA Trial Court opinion "appears to proceed from the assumption that FISA constructed a barrier between counterintelligence/intelligence officials and law enforcement officers" and that "[t]he [FISA Trial Court] apparently believes it can approve applications for electronic

deeper. The FISA Trial Court's reasoning ignores the whole point of the minimization procedures.

The minimization procedures do not balance the gathering of foreign intelligence information, on the one hand, against the gathering of evidence of crime, on the other hand. Rather, the minimization procedures balance the government's need to gather foreign intelligence information and use it for foreign intelligence purposes, on one side of the scales, against the privacy interests of U.S. persons, on the other side. The definition of minimization procedures reflects this balancing when it provides for procedures to minimize the acquisition and retention of information about U.S. persons, and to prohibit its dissemination, only to the extent "consistent with" the government's "need . . . to obtain, produce, and disseminate foreign intelligence information."[595] The government's "need" is a given, and minimization procedures must be designed to accommodate it.

This raises the question of why the government needs foreign intelligence information. The answer comes from the FISA's definition of "foreign intelligence information."[596] The definition of "foreign intelligence information" says the government needs this information because, if it concerns a U.S. person, it is necessary for five purposes. It is

> (1) . . . necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power;
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) . . . 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.

---

surveillance only if the government's objective is *not* primarily directed toward criminal prosecution of the foreign agents for their foreign intelligence activity.").

[595] 50 U.S.C. § 1801(h)(1) (2003).

[596] *Id.* § 1801(e).

The definition of minimization procedures refers to the government's "need" to "obtain, produce, and disseminate foreign intelligence information."[597] That "need" exists, however, only because that information is "necessary to" the five foreign intelligence purposes identified in the definition of foreign intelligence information.[598] If those purposes can be served by the use of FISA-acquired information for prosecutorial purposes, then minimization procedures must be consistent with the government's need to make such prosecutorial use of the information. Therefore, a set of proposed minimization procedures cannot be invalidated merely because they facilitate prosecutorial use. Yet that is the ground on which the FISA Trial Court rejected the Attorney General's 2002 procedures for consultation between intelligence officials and prosecutors.[599] The Court's decision conflicts with the definitions of "minimization procedures" and "foreign intelligence information," which require minimization procedures to accommodate foreign intelligence purposes.[600]

More broadly, these definitions reflect that the government can obtain, produce, and disseminate foreign intelligence information—

---

[597] *Id.* § 1801(h)(1).

[598] *Cf. In re* Sealed Case, 310 F.3d at 727 (rejecting the notion that "the government seeks foreign intelligence information (counterintelligence) [merely] for its own sake—to expand its pool of knowledge").

[599] *See In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 623 (Foreign Int. Surv. Ct. 2002) (finding Attorney General's 2002 procedures invalid because, and to the extent that, they "are designed to enhance the acquisition, retention, and dissemination of *evidence for law enforcement purposes, instead* of being consistent with the need of the United States to 'obtain, produce, and disseminate *foreign intelligence information*'").

[600] Professor Swire appears to endorse the FISA Trial Court's reliance on the portion of the FISA's text referring to "the need to obtain, produce, and disseminate foreign intelligence information." Swire, *supra* note 3, at 1337–38). Professor Swire, like the Trial Court, appears to treat the fulfillment of that need as the ultimate and the only legitimate purpose for FISA surveillance. *See id.* If I understand his view correctly, I respectfully disagree with it. For reasons explained in the text, the need to obtain produce, and disseminate foreign intelligence surveillance is not the ultimate purpose of FISA surveillance. To the contrary, that need exists only because of the government's need to achieve the five foreign intelligence purposes identified in the FISA's definition of "foreign intelligence information," which include purposes relating to protecting the United States from foreign attacks and other threats. Those are, in my view, the ultimate purposes for FISA surveillance. Based on that view, this article has argued that the three protective foreign intelligence purposes can, and under the original FISA may, be furthered by the prosecutorial use of FISA-acquired evidence. Neither Professor Swire nor the FISA Trial Court addresses this argument, apparently because they fail to identify the significance of the foreign intelligence purposes identified in the FISA's definition of foreign intelligence information. *See also infra* note 676 (explaining that Professor Swire's proposed amendment of FISA apparently loosens standard for FISA surveillance of U.S. persons).

and, of course, can use the information for foreign intelligence purposes—even though those activities disturb the privacy interests of U.S. persons. The activities merely must take place "in accordance with" procedures that minimize the disturbance.[601] Those activities include, but are not limited to, the use of information about U.S. persons to investigate and prosecute crime, when doing so serves foreign intelligence purposes. As explained in Part I, the government can make two other uses of information about U.S. persons, even though those uses may impinge on privacy interests. First, the government can temporarily acquire and retain information about U.S. persons, and disseminate it on a limited basis, to evaluate that information or other information that may be foreign intelligence information.[602] The government can use information for this evaluative purpose even though that use may not, strictly speaking, be directly "necessary to" a foreign intelligence purpose.[603] In addition, the government can use information about U.S. persons "that is evidence of a crime . . . for law enforcement purposes," whether or not that use serves a foreign intelligence purpose.[604] Thus, the government can use FISA-acquired information about U.S. persons, despite the use's intrusion on those persons' privacy interests, not only for foreign intelligence purposes but also for closely related evaluative purposes and purely for law enforcement purposes. All such uses simply must be carried out in ways that reasonably minimize their intrusiveness.

The FISA Trial Court would have had a statutory leg to stand on if it had invalidated the Attorney General's 2002 procedures because they were not "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate

---

[601] *See* 50 U.S.C. § 1806(a) (2003) ("Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter.").

[602] *See id.* §§ 1801(h)(1)–(2), discussed *supra* notes 139–59 and accompanying text.

[603] *See supra* notes 146–56 and accompanying text.

[604] *See* 50 U.S.C. § 1801(h)(3) (2003) (providing for minimization procedures that "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes"), discussed *supra* notes 143, 157–59 and accompanying text.

foreign intelligence information."[605] Instead, the court invalidated the procedures because, in its view, they favored the use of FISA-acquired information for law enforcement purposes over the gathering and processing of foreign intelligence. That view fundamentally misconceived the balancing of interests that Congress intended to strike with minimization procedures.[606]

b. Legislative History of Minimization Procedures

The legislative history of the minimization procedures confirms that the government can use information that has been obtained through FISA surveillance and that concerns U.S. persons for three sets of purposes: (1) for one or more of the foreign intelligence purposes identified in the definition of "foreign intelligence information"; (2) for the limited purpose of evaluating the information itself or other information that may be foreign intelligence information; and (3) for prosecutions even of crimes that do not relate to a foreign threat and even if the prosecutions themselves are not intended to advance any foreign intelligence purposes.

(1) The permissibility of using FISA-acquired information for one of the five foreign intelligence purposes identified in the definition of "foreign intelligence information" may be less obvious in the text of the FISA, as enacted, than it was in the bills that became the FISA. As enacted, Section 1806 of the original FISA said (and continues to say) that information obtained in FISA surveillance "may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter."[607] Section 1806 does not

---

[605] *Id.* § 1801(h)(1).

[606] This analysis does not deny differences between procedures designed to facilitate the use of information for law enforcement purposes and procedures designed to facilitate the use of information for advancing foreign intelligence purposes in other ways. *See, e.g.*, S. REP. NO. 95-701, at 14 (1978) (referring to "[t]he differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities"). For example, procedures to facilitate the gathering of evidence of crime should address matters, such as the chain of custody for physical evidence and the hearsay nature of statements, that do not bear directly on the gathering or processing foreign intelligence. Conversely, procedures to facilitate the gathering and processing of foreign intelligence should emphasize matters, such as protecting the identity of intelligence sources and methods, that do not bear directly on the concerns of the prosecutor. None of these concerns—neither the facilitation of prosecution nor the facilitation of foreign intelligence gathering and processing—underlie the provisions in the FISA on minimization procedures.

[607] FISA § 1806(a) (1978); 50 U.S.C. § 1806(a) (2003) (emphasis added).

expressly authorize (or prohibit) the use of FISA-acquired information to achieve the foreign intelligence purposes identified in the definition of "foreign intelligence information." That is because neither Section 1806 nor the definition of "minimization procedures" in Section 1801(h) mentions the foreign intelligence purposes that are identified in Section 1801(e)'s definition of "foreign intelligence information."[608] In contrast, as introduced, Section 1806 of the House and Senate bills that became the FISA expressly allowed information that had been obtained through FISA surveillance to be used for foreign intelligence purposes. The bills said that FISA-acquired information could be used "only for purposes specified in [the provision of the bill that defined 'minimization procedures'] or for the enforcement of the criminal law if its use outweighs the possible harm to the national security."[609] The bill's definition of "minimization procedures" articulated foreign intelligence purposes that were essentially identical to the foreign intelligence purposes specified in the bill's definition of "foreign intelligence information."[610] Thus, the bills articulated a set of foreign intelligence purposes in both the definition of minimization procedures and the definition of foreign intelligence information. By that redundancy, the version of Section 1806 in those bills expressly authorized the use of FISA-acquired information for foreign intelligence purposes.

As enacted, however, the FISA eliminated this redundancy by eliminating the specification of foreign intelligence purposes from the definition of minimization procedures. The legislative history does not explain why the reference was eliminated, but the reason does not seem to bear directly on the issues addressed here.[611] Unfortunately,

---

[608] 50 U.S.C. § 1801(e)–(h) (2003).

[609] S. 1566, 95th Cong. § 2526(a) (1977), *reproduced in Senate Judiciary Hearing on FISA*, *supra* note 70, at 151; S. REP. NO. 95-604 (1978) ("The bill would limit the use of information concerning United States citizens and lawful resident aliens acquired from electronic surveillances to matters properly related to foreign intelligence and the enforcement of criminal law."). The provision permitting FISA-acquired information to be used for law enforcement purposes was later taken out of § 1806, the provision addressing permissible uses, and put into the definition of minimization procedures in § 1801. *See* H.R. CONF. REP. NO. 95-1720, at 4, 22–23 (1978). At the same time, Congress removed the explicit requirement that the use of information "for the enforcement of the criminal law . . . outweigh[] the possible harm to the national security." The conference report explained that, "even without a statutory requirement, there will be an appropriate weighing of criminal law enforcement needs against a possible harm to the national security." *Id.* at 30.

[610] S. 1566, *supra* note 609, § 2521(b)(5), *reproduced in FISA of 1977: Hearings Before the Senate Judiciary Comm.*, 95th Cong. at 135–36.

[611] Early versions of the bills did not expressly allow information that had been obtained through FISA surveillance and that concerned U.S. persons to be retained and

however, the revision prevents the FISA, as enacted, from explicitly authorizing FISA-acquired information actually to be used for foreign intelligence purposes. That is nonetheless a permissible use of FISA-acquired information for reasons already discussed: The "need of the United States to obtain, produce, and disseminate foreign intelligence," to which the FISA's definition of "minimization procedures" refers, exists only because such intelligence is (if it concerns a U.S. person) "necessary to" one or more of the five foreign intelligence purposes identified in the FISA's definition of foreign intelligence information.[612]

(2) The second category of permissible uses of FISA-acquired information encompasses temporary acquisition and retention, and limited dissemination, of information for the purpose of evaluating it and other information that might be foreign intelligence information; this category is discussed primarily in the committee reports. The relevant discussions were noted in Part I.[613] Most importantly, the reports clarify that the acquisition, retention, and limited dissemination of even some information that is not itself "foreign intelligence information" may be "consistent with" the United States' need to gather and process foreign intelligence information.[614] That is because electronic surveillance cannot identify foreign intelligence information perfectly and instantaneously, as Congress knew.[615] Rather, it may take time for the government to learn whether information is "foreign intelligence information" or not.[616] This process often requires consideration of one piece of information in relation to other pieces. A piece of information may not be

---

disseminated for the limited purposes of determining whether it or other information was foreign intelligence information and, if so, understanding and assessing its importance. *See* S. REP. NO. 95-701, at 59 (1978) ("[T]he lawful uses of foreign intelligence information concerning U.S. citizens and resident aliens gathered pursuant to this chapter are restricted carefully to actual foreign intelligence purposes and the enforcement of the criminal law."); S. REP. NO. 95-604, at 37–39 (1978) (explaining that, as reported by the Senate Judiciary Committee, S. 1566 allowed information obtained through FISA surveillance to be used only for "one of the approved purposes" i.e., the foreign intelligence purposes specified in the definition of "foreign intelligence information" or "for enforcement of the criminal law"); *id.* at 53 (same). Congress may have amended the bills to clarify that the FISA permits temporary retention and evaluation of information that is not foreign intelligence information.

[612] *See supra* notes 596–600 and accompanying text.

[613] *See supra* notes 147–50.

[614] *See supra* notes 148–49.

[615] *See, e.g.*, S. REP. NO. 95-701, at 39 (1978) ("It is obvious that no electronic surveillance can be conducted so that innocent conversations can be totally eliminated.") (internal quotation marks omitted; footnote omitted).

[616] *See, e.g.*, H.R. REP. NO. 95-1283, pt. 1, at 58–59 (1978) (explaining that it may take time for relevance of information to become apparent).

"necessary" to a foreign intelligence purpose but may still be needed to identify, understand, or evaluate the importance of other information that is necessary to a foreign intelligence purpose.

(3) The third category of permissible uses of FISA-acquired information encompasses the use of FISA-acquired information "for law enforcement purposes" and is at once the trickiest and most relevant. As discussed above, the legislative history contains evidence of Congress's understanding that prosecutions can serve a foreign intelligence purpose.[617] That evidence is not found, however, in the legislative history on the minimization procedures. To the contrary, the legislative history on the minimization procedures contains at least one passage implying that Congress distinguished foreign intelligence purposes from law enforcement purposes. The passage concerns the FISA provision that is codified as § 1801(h)(3) and that requires minimization procedures to include procedures for the retention of information "that is evidence of a crime" for "law enforcement purposes":

> Paragraph (3) of the definition [of minimization procedures] relates to information which is evidence of a crime . . . . The committee felt . . . that it should be recognized in the definition of minimization procedures and the procedures themselves that the procedures do not bar retention and dissemination of evidence of a crime. As noted above, [in the report's discussion of the definition of "foreign intelligence information,"] evidence of certain crimes like espionage would itself constitute "foreign intelligence information, as defined, because it is necessary to protect against clandestine intelligence activities by foreign powers or their agents. Similarly, much information concerning international terrorism would likewise constitute evidence of crimes and also be "foreign intelligence information," as defined. This paragraph does not relate to information, even though it constitutes evidence of a crime, which is also needed by the United States in order to obtain, produce, or disseminate foreign intelligence information. For example, in the course of a surveillance evidence of a serious crime totally unrelated to intelligence matters might be incidentally acquired. Such evidence should not be required to be destroyed. Where the information is not foreign intelligence information, however, retention and dissemination of such evidence is allowed only to prevent the crime or to enforce the criminal law. Thus, this paragraph is not a loophole by which the Government can generally keep and disseminate derogatory information about individuals which may be a technical violation of law, where there is no intent actually to enforce the criminal law. On the other hand,

---

[617] *See supra* notes 358–60 & 559–60 and accompanying text.

> where the evidence also constitutes "foreign intelligence information," as defined, this paragraph does not apply, and the information may be disseminated and used for purposes other than enforcing the criminal law.[618]

This passage's last sentence, and especially the last sentence's use of the phrase "other than" (instead of "in addition to"), implies that the purposes for which foreign intelligence information is used are purposes "other than enforcing the criminal law."

The passage ultimately resists understanding because it does not indicate what those "other" purposes for obtaining foreign intelligence might be.[619] Instead, it observes that evidence of espionage is "necessary to protect" against clandestine intelligence activities without identifying how that protection will come about and without acknowledging that the government's mere possession of the evidence has little protective effect.[620] The passage also refers to information that is both evidence of crime and "is also needed by the United States in order to obtain, produce, or disseminate foreign intelligence information."[621] This reference presumably means that some information can be collected, retained, and disseminated for the purpose of evaluating it or other information that may be foreign intelligence information, and then used for prosecution. Such information would meet the "consistent with" standard in the first part of the definition of "minimization procedures"[622] and would be fit "for law enforcement purposes" under the third part of that definition.[623] But the passage does not recognize that information can fit the definition of "foreign intelligence information" because its use for investigation and prosecution serves a foreign intelligence purpose. For that reason, read in isolation, the passage arguably supports the judicial primary purpose test, which assumes an

---

[618] H.R. REP. NO. 95-1283, pt. 1, at 62 (1978).

[619] *Id.*

[620] *Id.*; *see also* 2003 Attorney General's Guidelines for FBI National Security Investigations, *supra* note 316, at 2 (redacted version) (describing "a variety of measures to deal with threats to the national security," including "arresting and prosecuting the perpetrators," as well as "recruitment of double agents and other assets; excluding or removing persons involved in terrorism or espionage from the United States; freezing assets of organizations that engage in or support terrorism; securing targets of terrorism or espionage; providing threat information and warnings to other federal agencies and officials, state and local governments, and private entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism or other national security threats").

[621] H.R. REP. NO. 95-1283, pt. 1, at 62 (1978).

[622] *See* 50 U.S.C. § 1801(h)(1) (2003).

[623] *Id.* § 1801(h)(3).

incompatibility between foreign intelligence purposes and law enforcement purposes.

Unlike the passage quoted above, other passages of committee reports on the FISA do expressly recognize that the prosecutorial use of FISA-acquired information can further foreign intelligence purposes. One such passage was already quoted above; it comes from a House report's discussion of the protective foreign intelligence purposes identified in the FISA's definition of foreign intelligence purposes.[624]

Another passage comes from a Senate committee report. It emphasizes that the foreign threats against which the government seeks to protect the country can include "serious crimes."[625] The report then discusses ways in which the bill "departs from ordinary criminal law enforcement procedures."[626] First, unlike an ordinary search or arrest warrant, a FISA surveillance order can issue without evidence of actual crime—even if, for example, a person's conduct only "may involve" a crime.[627] The report continues, "Additionally, surveillances conducted under [the bill] 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."[628]

The passage's reference to "protective measures other than arrest and prosecution" implies that "arrest and prosecution" are among the measures that can protect the country from foreign threats and thereby advance foreign intelligence purposes. In light of this passage and others recognizing that law enforcement uses of FISA-acquired

---

[624] *In re* Sealed Case, 310 F.3d 717, 724–25 (Foreign Int. Surv. Ct. Rev. 2002) (quoting H.R. REP. NO. 95-1283, pt. 1, at 49 (1978)) (ellipses and alteration in original) (emphasis removed):

> How this information may be used "to protect" against 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 . . . . And no information acquired pursuant to this bill could be used for other than lawful purposes . . . . Obviously, use of "foreign intelligence information" as evidence in a criminal trial is 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 [these activities] can be sought, retained, and used pursuant to this bill.

Id.

[625] S. REP. NO. 95-701, at 11 (1978).

[626] *Id.*

[627] *Id.*

[628] *Id.*

information can serve foreign intelligence purposes,[629] the murky passage from the House report quoted above is not strong evidence that Congress intended to prevent the government from using FISA surveillance to investigate and prosecute crime.[630]

C. Statutory Analysis of the Patriot Act

The FISA Court of Review put two limits on the government's use of FISA surveillance for prosecution. First, the government cannot use FISA surveillance for the primary (much less the sole) purpose of prosecuting non-foreign intelligence crimes.[631] The court traced that limit to the original FISA and rejected the argument that the Patriot Act removed the limit.[632] As discussed above, the Court of Review erred in construing the original FISA to impose that limit.[633] The Court of Review traced the second limit on the government's prosecutorial use of FISA surveillance to the Patriot Act.[634] The court held that under that Act the government cannot use FISA surveillance for the sole purpose of prosecuting foreign intelligence crimes.[635] This supposed restriction stems from the provision in Patriot Act that amends the original FISA's purpose provision to change the phrase "the purpose" to "a significant purpose."[636]

The court interpreted the "significant purpose" amendment, coupled with the coordination provision added by the Patriot Act, "clearly [to] disapprove the primary purpose test."[637] It then reasoned:

> [I]f a FISA application can be granted even if "foreign intelligence" is only a significant—not a primary—purpose, another purpose can be primary. One other legitimate purpose that could exist is to prosecute a target for a foreign intelligence crime. We therefore believe the Patriot Act amply supports the

---

[629] *See supra* notes 358–60, 559–60 and accompanying text; *see also* H.R. REP. NO. 95-1283, pt. 1, at 43 (1978) ("One might wonder why the Government would not immediately arrest [known international terrorists]. In some cases . . . it may be more fruitful in terms of combating international terrorism to identify otherwise unknown terrorists here, their international support structure, and the location of their weapons or explosives.").

[630] *Cf.* Zweibon v. Mitchell, 516 F.2d 594, 691 n.11 (D.C. Cir. 1975) (Wilkey, J., concurring and dissenting) (concluding that "the State Department viewed criminal prosecutions as one potentially effective means of achieving its overriding goal of maintaining good relations with the Soviet Union").

[631] *See In re* Sealed Case, 310 F.3d 717, 735–36 (Foreign Int. Surv. Ct. Rev. 2002).

[632] *See id.* at 736.

[633] *See supra* notes 500–04 and accompanying text.

[634] *See In re* Sealed Case, 310 F.3d at 734–36.

[635] *See id.* at 735.

[636] *See id.*

[637] *Id.* at 734; *see also id.* at 722 (describing government's alternative argument).

> government's alternative argument [i.e., that the Patriot Act eliminated the primary purpose test] but, paradoxically, the Patriot Act would seem to conflict with the government's first argument [i.e., that the distinction between foreign intelligence purposes and law enforcement purposes underlying the primary purpose test is "an illusion"] because by using the term "significant purpose," the Act now implies that another purpose is to be distinguished from a foreign intelligence purpose.[638]

The court found that Congress intended to "distinguish[] from a foreign intelligence purpose" the purpose of obtaining evidence for a prosecution. Accordingly, the Court of Review concluded: "The addition of the word 'significant' to [the original FISA's purpose provision] imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes." [639] Thus, the government cannot use FISA surveillance if its purpose is "just criminal prosecution of . . . foreign intelligence crimes."[640] The Court of Review's analysis is correct up to a point but wrong in the end.

The Court of Review correctly concluded that the legislative history of the Patriot Act expresses Congress's intent to strike a compromise.[641] On the one hand, Congress wanted to grant the government's request to eliminate the primary purpose test. On the other hand, Congress did not make the precise change to the original FISA's purpose provision that the government proposed because Congress wanted to give something to supporters of the primary purpose test. The big question is, what was the "something" that Congress gave supporters of the primary purpose test when it added the word "significant" to the original FISA's purpose provision? The Court of Review concluded that the addition ratified what would otherwise be a false distinction between foreign intelligence and law enforcement.[642] The court may well have been correct in believing that to be Congress's intent.[643] Even so, the Patriot Act should not be

---

[638] *Id.; see also id.* at 721–22 (describing government's first argument).

[639] *Id.* at 735.

[640] *Id.*

[641] *See supra* note 298 and accompanying text.

[642] *See In re* Sealed Case, 310 F.3d at 735 ("[E]ven though we agree that the original FISA did not contemplate the 'false dichotomy,' the Patriot Act did—which makes it no longer false. The addition of the word 'significant' . . . imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes. . . . Congress accepted the dichotomy between foreign intelligence and law enforcement by adopting the significant purpose test.").

[643] *See* 147 CONG. REC. S10593 (daily ed. Oct. 11, 2001) (colloquy between Sen.

interpreted as establishing that intent for three reasons.

First, it conflicts with the text of the FISA. Contrary to the Court of Review's description, the FISA's purpose provision, as amended by the Patriot Act, does not say that "a FISA application can be granted even if 'foreign intelligence' is only a significant—not a primary—purpose."[644] It says that a FISA application can be granted if "obtain[ing] foreign intelligence information" is only a significant, not a primary, purpose. The statute recognizes—whereas the Court of Review ignored—that "foreign intelligence" is not a purpose; obtaining foreign intelligence information, in contrast, is a purpose. More specifically, it is the purpose of obtaining a particular type of information (i.e., foreign intelligence information), rather than some other type of information. Thus, the FISA's purpose provision, as amended by the Patriot Act, continues to specify the type of information that the government must intend to obtain, and it does not explicitly address the government's intended use of that information. In isolation, the provision might be interpreted to allow the government to seek FISA surveillance for foreign intelligence information, as well as other types of information, as long as obtaining foreign intelligence information was a significant purpose of the proposed surveillance. The provision is not, however, grammatically susceptible of an interpretation that would cause it to distinguish between, on the one hand, the government's intended use of the information for law enforcement purposes and, on the other hand, the government's intended use of the information for "a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes."[645]

Nor is the provision susceptible of such an interpretation in the context of the FISA as a whole. As discussed above, although the original FISA's purpose provision did not explicitly address the government's intended use of the information sought under proposed FISA surveillance, the provision did address this issue implicitly.[646] It implied that the government must intend to use the information for one or more of the five foreign intelligence purposes identified in the FISA's definition of "foreign intelligence information."[647] It implied, further, that the achievement of foreign intelligence purposes had to

---

Cantwell and Sen. Leahy demonstrating that both senators distinguished surveillance for gathering foreign intelligence from surveillance for evidence of crime).

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

[645] *Id.* at 735.

[646] *See supra* notes 132–38 & 474–91 and accompanying text.

[647] *See supra* notes 476–82 and accompanying text.

be the government's "primary purpose" for seeking the information. Thus, the government could not seek a FISA surveillance order to pursue prosecution as an end in itself. But nothing in the text of the original FISA prevented the government from seeking FISA information for a prosecution that was intended to serve (and believed necessary to achieve) a foreign intelligence purpose. The original FISA did not prescribe the means by which the government had to use FISA-acquired information for a foreign intelligence purpose (other than to require that the use of such information, if it concerned U.S. persons, be "necessary" to achieving a foreign intelligence purpose and that the process of obtaining and using the information intrude on privacy concerns as little as reasonably possible). As amended by the Patriot Act, the FISA continues to leave largely to the executive branch the determination of how FISA-acquired information is to be used to achieve foreign intelligence purposes. In enacting the original FISA, Congress recognized that prosecutions could serve protective foreign intelligence purposes. Nothing in the text or legislative history of the Patriot Act suggests that, in the wake of 9/11, Congress forgot about the potential protective function of prosecution. Accordingly, the government can satisfy the current purpose provision of the FISA (just as it could satisfy the original FISA's purpose provision) if the government intends to use the information sought for a prosecution that the government intends to serve (and believes necessary to) a foreign intelligence purpose. That is true even if the government's *sole* purpose is to get evidence for that prosecution.[648] The FISA Court of Review's contrary conclusion conflicts with the text of the FISA.

The Court of Review's conclusion also conflicts with the purpose of the Patriot Act. The court recognized this when it described its conclusion as "paradoxical[]."[649] The paradox is that, under the court's interpretation, the Patriot Act creates, for the first time, a statutory basis for distinguishing, in the context of FISA surveillance, between foreign intelligence purposes and law enforcement purposes. This is the very distinction upon which the wall rested.[650] The Court of Review found no basis for the distinction in the original FISA and concluded that it was introduced by the Patriot Act.[651] Yet the

---

[648] *See supra* notes 492–516 and accompanying text.

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

[650] *See supra* notes 171–262 and accompanying text.

[651] *In re* Sealed Case, 310 F.3d at 735 ("The addition of the word 'significant' to section 1804(a)(7)(B) [of the FISA] imposed a requirement that the government have a

original FISA was enacted to restrict the government's surveillance powers while the Patriot Act was designed to expand them.[652] Under the Court of Review's interpretation of the purpose provision, the original FISA's version was less restrictive of government surveillance power than the post-Patriot Act version. The counterintuitiveness of the court's interpretation does not, standing alone, justify rejecting it; it is not an absurd result. But the counterintuitiveness of the interpretation is relevant when coupled with the analysis above showing that the court's interpretation conflicts with statutory text.

For the same reason, it matters that the FISA Court of Review attributed logical precision to Congress that seems unwarranted considering the circumstances of the Patriot Act's passage. The Court of Review interpreted the FISA, as amended by the Patriot Act, to distinguish among (1) FISA surveillance undertaken with the "sole objective" of prosecuting "foreign intelligence crimes";[653] (2) FISA surveillance for the "primary" purpose of prosecuting "foreign intelligence crimes";[654] (3) FISA surveillance for the primary purpose of prosecuting "ordinary crimes . . . inextricably intertwined with foreign intelligence crimes";[655] and (4) FISA surveillance for the primary or sole purpose of prosecuting all other "ordinary crimes."[656] Those distinctions lack any anchor in the text of the FISA, which does not define "foreign intelligence crimes," and the scant legislative history of the Patriot Act's hurried enactment does not evince congressional appreciation of those distinctions.[657]

---

measurable foreign intelligence purpose other than just criminal prosecution of even foreign intelligence crimes.").

[652] *See supra* notes 60–71 & 287–304 and accompanying text; *see also, e.g., Senate Intelligence Hearing on FISA*, *supra* note 70, at 141 (reproducing letter to Sen. Inouye from George Hasen, Chairman, Comm. on Civil Rights, Ass'n of Bar of NYC) ("We think it is important to remember why this legislation is needed. Clearly it is not needed to empower government agencies to carry on electronic surveillance. Rather, the need is for legislation which will limit and control electronic surveillance.").

[653] *In re* Sealed Case, 310 F.3d at 735–36; *see also id.* at 723 & n.10 (defining "foreign intelligence crime"); *but cf. id.* at 736 (apparently amending definition of "foreign intelligence crime" to include "ordinary crimes . . . inextricably intertwined with foreign intelligence crimes").

[654] *See id.* at 734 (stating that a "legitimate purpose" for surveillance under FISA, as amended by the Patriot Act, is "to prosecute a target for a foreign intelligence crime," and that this purpose "can be primary"); *see also id.* at 723 & n.10 (defining "foreign intelligence crime"); *but cf. id.* at 736 (apparently amending definition of "foreign intelligence crime" to include "ordinary crimes . . . inextricably intertwined with foreign intelligence crimes").

[655] *Id.* at 736.

[656] *See id.* at 734–36; *see also supra* notes 350–409 and accompanying text.

[657] Congress enacted the Patriot Act six weeks after the 9/11 attacks; the legislation

Finally, there is a better alternative to the Court of Review's interpretation of the Patriot Act's amendments of the FISA. The alternative interpretation begins with the same understanding of the congressional intent behind the amendment as the Court of Review had: Congress wanted to scrap the primary purpose test, as the administration requested, while giving something to the supporters of the primary purpose test. More particularly, as the Court of Review recognized, Congress apparently wanted to "giv[e] the FISA court the authority [when reviewing a government application for a FISA surveillance order] to review the government's purpose in seeking the information."[658] This article has argued that the original FISA already gave courts that authority but did so only implicitly.[659] The Patriot Act's amendment of the purpose provision, coupled with the Patriot Act's addition of the coordination provision,[660] can be interpreted as making that authority explicit in the FISA for the first time. This change plainly favors supporters of the primary purpose test, which rests on the existence of judicial authority to review the government's purpose for seeking information under the FISA. Congress's use of the word "significant" instead of "primary," however, reflects an intent to allow less searching judicial review of the government's purpose than permitted under the primary purpose test.[661] Overall, the Patriot Act did achieve a compromise, though one much rougher than the intricate one suggested by the FISA Court of Review's interpretation.

The remaining substantive question is what purposes for FISA surveillance are impermissible? (There must be some impermissible purposes, or else it was pointless for Congress in the Patriot Act explicitly to authorize judicial review of the government's purpose.) This article has argued that the original FISA did not permit the government to use FISA surveillance for prosecution as an end in

---

produced no committee reports. *See In re* Sealed Case, 310 F.3d at 732 (noting absence of committee reports); 115 Stat. 272 (reflecting enactment date of Oct. 26, 2001).

[658] *In re* Sealed Case, 310 F.3d at 735.

[659] *See supra* notes 132–38 & 474–91 and accompanying text.

[660] *See supra* notes 302–03 and accompanying text (discussing "coordination" provision in 50 U.S.C. § 1806(k) (2003)).

[661] *See, e.g.*, 147 CONG. REC. S10591 (daily ed. Oct. 11, 2001) (statement of Sen. Feinstein) ("The effect of this provision will be to make it easier for law enforcement to obtain a FISA search or surveillance warrant for those cases where the subject of the surveillance is both a potential source of valuable intelligence and the potential target of a criminal prosecution."); *id.* at S10593 (statement of Sen. Leahy) (amendment would "make it easier for the FBI to use a wiretap where the Government's most important motivation for the wiretap is for use in a criminal prosecution").

itself.[662] That remains an impermissible purpose under the Patriot Act since, as was discussed above, the applicable analysis does not change.[663] Other impermissible purposes exist, under both the original FISA and the FISA as amended by the Patriot Act, but they do not involve prosecutorial use. Rather, they reflect Congress's intent in the original FISA to prohibit the abuses revealed by the Church Committee, which consisted of "national security" surveillance being conducted, and information obtained through such surveillance being used, for "political" and "personal" purposes that had no relationship to any legitimate government objective.[664] Although the original FISA implicitly authorized judicial review to ferret out such improper purposes, the Patriot Act amendments made the authority explicit (while relaxing it).[665]

D. Summary of Statutory Analysis

This Part concludes that the original and current versions of the FISA allow the government to use FISA surveillance to obtain evidence for prosecuting any type of crime if the government intends the anticipated prosecution to serve (and believes the anticipated prosecution to be necessary to) a foreign intelligence purpose. (The FISA identifies five eligible foreign intelligence purposes in defining "foreign intelligence information," the first three of which concern "protective" or "counter" intelligence and are therefore usually the purposes that will potentially be advanced by a prosecution.) Thus, lower federal courts have erred in interpreting the original FISA to impose the primary purpose test, and the FISA Trial Court erred in

---

[662] *See supra* notes 465 & 482 and accompanying text.

[663] *See supra* notes 644–48 and accompanying text.

[664] *See supra* notes 60–66 and accompanying text.

[665] *United States v. Truong Dinh Hung* illustrates the problem caused by judicial review under the judicial primary purpose test. In that case the court decided that as of a certain date the Department's investigation was "primarily" for prosecution purposes rather than foreign intelligence purposes. *See* 629 F.2d 908, 916 (4th Cir. 1980). This was easy for the court to say, with the benefit of hindsight and based on reviewing all of the relevant internal Justice Department memoranda. In the midst of the investigation, however, officials may often cross the invisible line without knowing or intending to do so, and only later have a prosecution crumble because of a court's post hoc determination of when they crossed the line. *See* William F. Brown and Americo R. Cinquegrana, *Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment*, 35 CATH. U. L. REV. 97, 144 (1985). On the other hand, as Professor Peter Raven-Hansen observed in commenting on a draft of this article, the Fourth Amendment could be understood to require the government to get a warrant based on traditional probable cause, once it has developed probable cause of crime and an intention to prosecute that crime. On that understanding, the showing that FISA requires for a surveillance order does not satisfy the Fourth Amendment.

interpreting the current FISA to do so. Contrary to that case law, the government may use FISA surveillance for the primary, and even the sole purpose of getting evidence for prosecution. The government must, however, intend the anticipated prosecution to serve a foreign intelligence purpose. The executive branch's judgment that a prosecution will serve such a purpose should receive great deference from reviewing courts.

Although the case law imposing the judicial primary purpose test misread the original and current FISA, so did the FISA Court of Review, in two ways. First, the Court of Review erred in construing the original and current FISA to prevent the government from using FISA surveillance for the primary (or sole) purpose of prosecuting "non-foreign intelligence crimes." Under the original and current FISA, the government can use foreign intelligence information sought in a proposed FISA surveillance order for the primary purpose of prosecuting any crime as long as the government intends the prosecution or some other intended use of the information to serve a foreign intelligence purpose. Second, the FISA Court of Review erred in construing the FISA, as amended by the Patriot Act, to prevent the government from using FISA surveillance for the sole purpose of prosecuting "foreign intelligence crimes."[666] The government may do so if it intends the prosecutions to serve a foreign intelligence purpose.

The analysis of the FISA offered in this Part puts one limit on the government's intended use of FISA surveillance solely for prosecution purposes: the government must intend the prosecution to serve a foreign intelligence purpose identified in the definition of "foreign intelligence information." That limit is not unique to prosecutorial uses of FISA-acquired information. Rather, it inheres in FISA's requirement that a high-ranking intelligence official certify that "the purpose" (under the original FISA) or "a significant purpose" (under the FISA as amended by the Patriot Act) of the proposed surveillance is to "obtain foreign intelligence information."[667] The FISA defines "foreign intelligence information," when it concerns U.S. persons, as information that is "necessary to" five foreign intelligence purposes.[668] Because of that instrumental definition, when the government certifies that it has a purpose of

---

[666] *In re* Sealed Case, 310 F.3d 717, 735 (Foreign Int. Surv. Ct. Rev. 2002).

[667] 50 U.S.C. § 1804(a)(7)(B) (2003).

[668] *Id.* § 1801(e); *see also supra* notes 98–102, 136–38, 477–82, 596–600 and accompanying text.

obtaining information "necessary" to a particular purpose, it implies that it intends to use the information for that purpose. When the government intends to use information for prosecution, it must intend that prosecution to serve a foreign intelligence purpose. The same is true for whatever use the government intends to make of the information sought through proposed FISA surveillance; the use must be intended to serve a foreign intelligence purpose. This conclusion flows from the purpose provision coupled with the definition of foreign intelligence information.

The statutory analysis offered here distinguishes the government's intended use of the information sought under a proposed FISA surveillance order from the government's actual use of the information so obtained. The government must intend to use the information for a foreign intelligence purpose. Electronic surveillance for foreign intelligence, however, does not operate perfectly and instantaneously. As a result, while the government may intend surveillance to produce only foreign intelligence information, actual surveillance may produce information that is hard to classify. Accordingly, the FISA allows the government temporarily to retain and disseminate on a limited basis information acquired under the FISA for the limited purposes of evaluating it and other information that may turn out to be foreign intelligence information. In addition, the FISA allows the government to use information that is evidence of a crime "for law enforcement purposes," even if that information is not foreign intelligence information, i.e., even if its use would not serve a foreign intelligence purpose.[669]

The statutory analysis offered here gives the government broad power to use foreign intelligence information obtained through FISA surveillance, but the government's purpose must be to obtain information that is indeed "foreign intelligence information." Accordingly, if the information sought concerns U.S. persons, courts can review the government's determination that the information sought is foreign intelligence information because its intended use (for prosecution or other purposes) serves one of the foreign intelligence purposes identified in the definition of "foreign intelligence information." Specifically, FISA empowers a FISA judge to review for clear error the government's certifications "(A) that the certifying official deems the information sought to be foreign intelligence information; [and] (B) that the purpose of the surveillance

[669] *Id.* §§ 1801(h)(3), 1806(a).

is to obtain foreign intelligence information."[670] Further judicial review can occur if the government seeks to use information obtained through FISA surveillance in a criminal proceeding.[671] Based on experience under the FISA, this review will seldom, if ever, lead to judicial invalidation of FISA surveillance.[672] The review does, however, limit the government's ability to use FISA surveillance for the improper purposes that were revealed by the Church Committee and that influenced the original passage of the FISA.[673]

The proposed statutory analysis treats the Patriot Act amendments of the FISA as benefiting both supporters of the primary purpose test and the government, which sought elimination of the test. The Patriot Act benefited supporters of the test by making explicit in the FISA, for the first time, the courts' authority to review the government's intended use of information sought through FISA surveillance. The Patriot Act benefited the government by eliminating the primary purpose test except insofar as the test reflected the existence of judicial power to review the government's intended use of information sought through FISA surveillance.

IV. AN ARGUMENT FOR A STATUTORY CLARIFICATION THAT ARGUABLY MAKES A SUBSTANTIVE CHANGE TO THE FISA

The first three parts of this article explain what the original and current versions of the FISA mean. It is hoped that the article both clarifies the meaning of the relevant statutory provisions and also (through the article's length if nothing else) proves the need for congressional clarification. As to how the statutes should be clarified, this article offers a suggestion, while recognizing (without lengthily defending) its arguably substantive effect.[674]

---

[670] *Id.* § 1804(a)(7); *see also id.* § 1805(a)(5).

[671] *See id.* §§ 1806(b)–(g) (prescribing procedures for use of FISA-acquired information in a criminal proceeding).

[672] *See supra* note 225 and accompanying text (observing that courts have not, in any published decision, used the "primary purpose" test to suppress FISA-acquired or FISA-derived evidence from a criminal proceeding).

[673] *See Senate Intelligence Hearing on FISA*, *supra* note 42, at 197–98 (discussing amendment to certification procedures that would require judicial review of whether information sought under proposed surveillance order actually is foreign intelligence information, rather than merely reviewing whether certifying official deemed it such); *id.* at 222–23 (statement of Sen. Bayh) (similar description).

[674] I recognize, as well, that the proposed clarification would not solve systemic problems. Senators Patrick Leahy, Charles Grassley, and Arlen Specter, *Interim Report on FBI Oversight in the 107th Cong. by the Sen. Judiciary Comm.* at § III.C.3.b.ii (Feb. 2003) (observing, with reference to FBI's implementation of the FISA, that changes to legislation often cannot solve problems in an agency's implementation of existing

Congress should amend the FISA's definition of "foreign intelligence information" to add the language italicized below:

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

This amendment would clarify that the government can use investigation, arrest, prosecution and other law-enforcement means to achieve the three protective foreign intelligence purposes identified in the portion of the definition of foreign intelligence information that concerns "protective" or "counter" intelligence.[675]

The amendment would not amend the portion of the definition that concerns "positive" (also known as "affirmative" or just plain) intelligence. That is because prosecution is not a usual method of maintaining "the national defense or the security of the United States" or of "conduct[ing] . . . foreign affairs." The amendment would not prevent the government from arguing in a particular situation, however, that an intended prosecution was necessary to national defense or national security or was necessary to the United States's conduct of foreign affairs. Usually, however, prosecutions will either serve one or more of the three protective foreign intelligence purposes or they will have no "necessary" relationship to any foreign

---

statutes), *available at* http://www.fas.org/irp/congress.2003_rpt/fisa.html; *see also* 9/11 COMM'N REPORT, *supra* note 2, at 416–19 (calling for "unity of effort in sharing information" across the government).

[675] *See* H.R. CONF. REP. NO. 95-1720, at 23 (1978) (defining "law enforcement purposes" to include "arrest, prosecution, and other law enforcement measures taken for the purpose of preventing the crime").

intelligence purpose.[676]

Although the amendment proposed above confirms the interpretation of existing statutes offered in this article, this amendment would change the FISA substantively, if one disagrees with the interpretation offered here. In particular, the amendment would strip away the restrictions imposed by (1) case law interpreting the original FISA's purpose provision to impose a "primary purpose" test; (2) the FISA Trial Court decision interpreting the FISA's provisions on minimization procedures to empower the court to require procedures that, in effect, impose the primary purpose test; and (3) the FISA Court of Review's decision, which prohibits the government from (a) using FISA surveillance for the primary or sole purpose of prosecuting "non-foreign intelligence crimes"; and (b) using FISA surveillance for the sole purpose of prosecuting "foreign intelligence crimes." This article will not rehearse the pros and cons of the primary purpose test, for those are well catalogued in the case law, the legislative history, and prior commentary. The article will instead briefly explain why Congress should eliminate the limits on government power imposed under the FISA Court of Review's decision.

One limit imposed by the Court of Review's decision requires government officials and the courts to draw a line between "foreign intelligence crimes" and "non-foreign intelligence crimes."[677] The executive and judicial branches must draw this line because Congress has not done so. The FISA does not use the terms "foreign intelligence crimes" or "non-foreign intelligence crimes"; they come solely from the FISA Court of Review's opinion. FISA's definitions of 'foreign intelligence information' and "agent of a foreign power' do usually implicate criminal activity, but they also may implicate

---

[676] Professor Swire proposes amending the FISA's purpose provision to require a certification that "the information sought is expected to be sufficiently important for foreign intelligence purposes to justify" the issuance of a FISA surveillance order. Swire, *supra* note 3, at 1364. This proposed amendment, as applied to surveillance targeting U.S. persons, could have the effect of broadening the government's power to conduct FISA surveillance. Currently, the FISA defines "foreign intelligence information" as information that, if it concerns U.S. persons, is "necessary" to one or more of five specific foreign intelligence purposes. 50 U.S.C. § 1801(e) (2003). A standard allowing the government to conduct FISA surveillance to obtain information that is "sufficiently important for foreign intelligence purposes" seems more lenient than a standard that allows the government to conduct FISA surveillance to obtain only that information which is "necessary" to specific foreign intelligence purposes. I would not favor Professor Swire's proposed amendment for that reason and because it appears to invite federal judges to second-guess executive branch judgments about the intelligence value of information sought under a FISA order.

[677] *In re* Sealed Case, 310 F.3d 717, 735–36 (Foreign Int. Surv. Ct. Rev. 2002).

conduct that is not always a crime, such as entering the country "under a false or fraudulent identity for or on behalf of a foreign power."[678] The FISA Court of Review classified this false or fraudulent conduct as a "foreign intelligence crime," even though the statute does not.[679] The court likewise fudged on the meaning of "non-foreign intelligence crimes," leaving unclear whether that term means (1) any crime that is not a "foreign intelligence crime," as defined by the court,[680] or (2) any crime that is not a "foreign intelligence crime," as defined by the court, plus otherwise "ordinary crimes" that, in particular instances, are "inextricably intertwined with foreign intelligence crimes."[681]

The court's own trouble drawing the line between "foreign intelligence crimes" and "non-foreign intelligence crimes" demonstrates the weakness of the distinction. For one thing, the distinction conflicts with congressional intent in the FISA. By defining foreign intelligence information to include some noncriminal conduct, Congress judged some noncriminal conduct worthy of government surveillance and perhaps further response. Second, the distinction is unjustified, because the prosecution of any crime can serve a foreign intelligence purpose when that crime is committed by a foreign power or its agent. Indeed, the 9/11 Commission's Report describes instances in which actual or suspected international terrorists committed crimes with no immediately obvious connection to their terrorist activities.[682] The government should be able to use FISA surveillance to investigate and prosecute those crimes, and thereby take terrorists off the street and in government custody. The arrest and news of their arrest can disrupt ongoing plans of violence.[683] Furthermore, in custody the government can do further

---

[678] *See* 50 U.S.C. § 1801(b)(2)(C) & (e); *see also* supra notes 89, 98–100, 111–116, 129, 554–576 and accompanying text.

[679] *In re* Sealed Case, 310 F.3d at 723 n.10.

[680] *Id.* at 723 ("For purposes of clarity in this opinion we will refer to the crimes referred to in section 1801(a)–(e) as foreign intelligence crimes."); *but cf. id.* at 723 n.10 (noting that the court's definition of "foreign intelligence crimes" also includes conduct described in 50 U.S.C. § 1801(b)(2)(D), "which will almost always involve a crime").

[681] *Compare In re* Sealed Case, 310 F.3d at 723 & n.10 *with id.* at 736.

[682] *See* 9/11 COMM'N REPORT, *supra* note 2, at 176–77 (discussing crimes, including "petty crime," that Ahmed Ressam committed while moving to, and living in Canada, before entering the United States with explosives for the planned millennium bombing); *id.* at 230 (reporting that Jordanian suspected of aiding two of the 9/11 hijackers while they were in the United States was deported to Jordan after 9/11, having been convicted of "a fraudulent driver's license scheme"); *see also id.* at 424 ("Counterterrorism investigations often overlap or are cued by other criminal investigations, such as money laundering or the smuggling of contraband.").

[683] *See, e.g.*, 9/11 COMM'N REPORT, *supra* note 2, at 276 (observing that publicity about

investigation (e.g., interrogation) that may uncover more foreign intelligence information, including evidence of what the Court of Review called "foreign intelligence crimes."[684]

The other limit imposed by the Court of Review prevents the use of FISA surveillance for the sole purpose of prosecuting even foreign intelligence crimes.[685] The court minimized the importance of this limit, emphasizing that the government could meet this restriction as long as, when applying for a FISA surveillance order, it "entertains a realistic option of dealing with the [United States person-foreign] agent other than through criminal prosecution."[686] This restriction may turn out to be trivial, since virtually all prosecutions are meant either generally or specifically to deter future misconduct. Yet to the same extent that the restriction is trivial, it is also arbitrary. The court adopted the restriction because it felt obliged to interpret the Patriot Act's "significant purpose" amendment in some way that distinguishes law enforcement objectives from foreign intelligence objectives.[687] As discussed above, however, one can agree with the Court of Review that Congress in the Patriot Act "accepted the dichotomy between foreign intelligence and law enforcement"[688] without interpreting the Act to incorporate that dichotomy, when such an interpretation cannot be shoehorned into any available statutory text and cannot be reconciled with the intent of the Patriot Act or the circumstances of its enactment.

V. CONCLUSION

The 9/11 attacks demand answers to why the United States did not prevent them. One factor cited has been "the wall" between foreign intelligence and law enforcement. The wall is almost as shadowy as were the forces behind the attacks. The wall resists understanding

---

the pre-9/11 arrest of Zacarias Moussaoui, the suspected "20th hijacker," "might have derailed the plot").

[684] *In re* Sealed Case, 310 F.3d at 723 & n.10. Federal jurisdiction over even petty crimes could be based on the status of the defendant as an agent of a foreign power and the government's national security purpose in prosecuting that defendant. *Cf.* Verlinden B.V. v. Central Bank of Nigeria, 461 U.S. 480, 491–97 (1983) (holding that Article III "arising under" clause allowed Congress to give federal courts jurisdiction over certain civil actions between foreign plaintiffs and foreign sovereigns where rule of decision may be provided by state law).

[685] *In re* Sealed Case, 310 F.3d at 735.

[686] *Id.*

[687] *See id.* ("Congress [in the Patriot Act] accepted the dichotomy between foreign intelligence and law enforcement by adopting the significant purpose test. . . . [I]t is our task to do our best to read the statute to honor congressional intent.").

[688] *Id.*

because it arose behind an intricate statutory framework that was implemented mostly in secret. Moreover, as the public learns more about the wall, it grows and multiplies beyond the set of barriers inside the Justice Department that originally were known as the wall. This article, however, focuses on "the wall" in its original denotation, as a set of restrictions on information sharing within the Department of Justice, including the FBI. The article concludes that this wall has never had a statutory foundation and still lacks one. To dispel the confusion on that score, Congress should clarify the matter when it debates reauthorization of the Patriot Act.